EMERGING THREATS: ASSESSING NUCLEAR WEAPONS COMPLEX FACILITY SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JUNE 24, 2003

Serial No. 108–62

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

89–848 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
WILLIAM J. JANKLOW, South Dakota
MARSHA BLACKBURN, Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
CHRIS BELL, Texas

BERNARD SANDERS, Vermont (Independent)

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

MICHAEL R. TURNER, Ohio
DAN BURTON, Indiana
STEVEN C. LATOURETTE, Ohio
RON LEWIS, Kentucky
TODD RUSSELL PLATTS, Pennsylvania
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
TIM MURPHY, Pennsylvania
WILLIAM J. JANKLOW, South Dakota

DENNIS J. KUCINICH, Ohio
TOM LANTOS, California
BERNARD SANDERS, Vermont
STEPHEN F. LYNCH, Massachusetts
CAROLYN B. MALONEY, New York
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
CHRIS BELL, Texas
JOHN F. TIERNEY, Massachusetts

EX OFFICIO

TOM DAVIS, Virginia
HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
KRISTINE MCELROY, *Professional Staff Member*
ROBERT A. BRIGGS, *Clerk*
MICHAEL YEAGER, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on June 24, 2003	1
Statement of:	
Brian, Danielle, executive director, Project on Government Oversight; and Ronald E. Timm, president, Reta Security	96
Brooks, Linton F., Administrator, National Nuclear Security Administration, Department of Energy; and Joseph S. Mahaley, Director, Office of Security, Department of Energy	52
Nazzaro, Robin M., Director, Natural Resources and Environment, U.S. General Accounting Office, accompanied by James Noel, Assistant Director, and Jonathan M. Gill, Evaluator, Natural Resources and Environment; and Glenn S. Podonsky, Director, Office of Oversight and Performance Assurance, U.S. Department of Energy	6
Letters, statements, etc., submitted for the record by:	
Brian, Danielle, executive director, Project on Government Oversight: Report entitled, "U.S. Nuclear Weapons Complex: Security at Risk"	98
Prepared statement of	153
Brooks, Linton F., Administrator, National Nuclear Security Administration, prepared statement of	57
Grassley, Hon. Charles, a Senator in Congress from the State of Iowa, prepared statement of	77
Mahaley, Joseph S., Director, Office of Security, Department of Energy, prepared statement of	71
Nazzaro, Robin M., Director, Natural Resources and Environment, U.S. General Accounting Office, prepared statement of	9
Podonsky, Glenn S., Director, Office of Oversight and Performance Assurance, U.S. Department of Energy, prepared statement of	34
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of	3
Timm, Ronald E., president, Reta Security, prepared statement of	163

EMERGING THREATS: ASSESSING NUCLEAR WEAPONS COMPLEX FACILITY SECURITY

TUESDAY, JUNE 24, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:07 a.m., in room 2247, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Turner, Lewis, Platts, Duncan, Ruppersberger, and Tierney.

Staff present: Lawrence Halloran, staff director and counsel; J. Vincent Chase, chief investiator; Kristine McElroy, professional staff member; Michael Yeager, minority deputy chief counsel; and Jean Gosa, minority assistant clerk.

Mr. SHAYS. A quorum being present, the Subcommittee on National Security, Emerging Threats and International Relations hearing, entitled, "Emerging Threats: Assessing Nuclear Weapons Complex Facility Security," is called to order.

From its humble beginnings as the Manhattan Project in the distant New Mexico desert, the Nation's nuclear weapons program has always posed daunting security challenges. Today, the far-flung complex of warhead production plants, research laboratories, test facilities, and former weapons sites stands as an undeniably attractive target for spies and terrorists bent on using their own technologies against us.

Even before the attacks of September 11, 2001 forced a reevaluation of physical security standards and procedures, serious questions arose concerning lax management and a stubborn cultural antipathy to protective measures at sites housing plutonium and highly enriched uranium. In response, Congress established the National Nuclear Security Administration [NNSA], as a semi-autonomous agency within the Department of Energy [DOE], to focus resources and high-level management attention on security mandates.

However, creation of the NNSA failed to stem persistent reports of security lapses and inattentiveness to lingering vulnerabilities throughout the weapons complex. So the subcommittee asked the General Accounting Office [GAO], to evaluate DOE and NNSA management of material safeguards and facility security programs. Of particular interest was how DOE assures contractor adherence to security policies.

The GAO findings released today lead to this sobering conclusion: The stern new realities of the post-September 11 world have been far too slow to penetrate the hardened bureaucratic maze of DOE offices, contractors and sites. It took 2 years for DOE to update the fundamental assessment governing nuclear weapons security. The design basis threat [DBT], formally adopted in May, the new, more stringent DBT will not be fully reflected in budget plans until 2005. More of concern, security enhancements demanded by the new DBT will not be completed before 2009, if then.

Even the process of completing the GAO study under discussion today was needlessly delayed by DOE refusal to provide access to drafts of the DBT, drafts openly relied upon to justify earlier budget submissions. DOE eventually provided the documents to Congress' audit agency, and we hope that level of cooperation will continue as we pursue our investigation.

GAO has found a lack of clear roles and responsibilities among NNSA security offices, inconsistent assessments of contractor performance, potentially critical staff shortfalls and a failure to address the root causes of security lapses. As a result, neither the Department of Energy nor the NNSA can yet provide reasonable assurance weapons grade material is protected against a determined, well-trained adversarial force willing to die in a nuclear detonation or radiological dispersion of their own making.

This morning, we will hear testimony on the process of updating and administering security standards at the Nation's nuclear weapons complex. Classified elements of the security and safeguards program will be discussed at a closed session this afternoon.

Our witnesses today all bring impressive experience and important expertise to our continuing oversight of nuclear security. They also share a dedication to improve national security and public safety, and we look forward to a constructive dialog on these important issues.

Before recognizing Mr. Turner, let me just apologize for being a little late. I got in to Andrews Air Force Base at about 2:30 last night.

[The prepared statement of Hon. Christopher Shays follows:]

TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
JOE DOE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382
E-mail: hr.groc@mail.house.gov

Statement of Rep. Christopher Shays
June 24, 2003

From its humble beginnings as the Manhattan Project in the distant New Mexico desert, the nation's nuclear weapons program has always posed daunting security challenges. Today, the far-flung complex of warhead production plants, research laboratories, test facilities, and former weapons sites stands as an undeniably attractive target for spies and terrorists bent on using our own technologies against us.

Even before the attacks of September 11, 2001 forced a reevaluation of physical security standards and procedures, serious questions arose concerning lax management and a stubborn cultural antipathy to protective measures at sites housing plutonium and highly enriched uranium. In response, Congress established the National Nuclear Security Administration (NNSA) as a semi-autonomous agency within the Department of Energy (DOE) to focus resources and high-level management attention on security mandates.

But creation of the NNSA failed to stem persistent reports of security lapses and inattentiveness to lingering vulnerabilities throughout the weapons complex. So the Subcommittee asked the General Accounting Office (GAO) to evaluate DOE and NNSA management of material safeguards and facility security programs. Of particular interest was how DOE assures contractor adherence to security policies.

The GAO findings released today lead to this sobering conclusion: The stern new realities of the post-9/11 world have been far too slow to penetrate the hardened bureaucratic maze of DOE offices, contractors and sites. It took two years for DOE to update the fundamental assessment governing nuclear weapons security – the Design Basis Threat or DBT. Formally adopted in May, the new, more stringent DBT will not be fully reflected in budget plans until 2005. Security enhancements demanded by the new DBT will not be completed before 2009, if then.

Even the process of completing the GAO study under discussion today was needlessly delayed by DOE refusal to provide access to drafts of the DBT; drafts openly relied upon to justify earlier budget submissions. DOE eventually provided the documents to Congress' audit agency, and we hope that level of cooperation will continue.

GAO also found a lack of clear roles and responsibilities among NNSA security offices, inconsistent assessments of contractor performance, potentially critical staff shortfalls and a failure to address the root causes of security lapses. As a result, neither the Department of Energy nor the NNSA can yet provide reasonable assurance weapons grade material is protected against a determined, well trained adversary force willing to die in a nuclear detonation or radiological dispersion of their own making.

This morning we will hear testimony on the process of updating and administering security standards at the nation's nuclear weapons complex. Classified elements of the security and safeguards program will be discussed at a closed session this afternoon.

Our witnesses today all bring impressive experience and important expertise to our continuing oversight of nuclear security. They also share a dedication to improved national security and public safety, and we look forward to a constructive dialogue on these important issues.

Mr. TURNER. Thank you, Mr. Chairman. I want to thank you again for your efforts and leadership in addressing the issue of our national security and the threats that are posed by issues of possible targets of terrorist attacks.

Our national labs and nuclear production facilities are appealing targets for terrorists. These sites are challenges to secure, spread over large parcels of land and containing some of the most deadly materials known to man. Terrorists now use once unimaginable tactics to cause death and destruction, and we must now account for the possibility that terrorists will sacrifice their own lives to carry out their missions. And the thought of terrorists attempting to steal plutonium or highly enriched uranium is no longer related to Tom Clancy novels, but is a real-life threat.

I am particularly interested in hearing how we can make the NNSA more responsive and flexible to the threats facing our weapons complexes, and it should not take months and years to develop security procedures. The real world does not work this way, terrorists do not work this way, and the ground-level security personnel do not think this way.

I look forward to hearing our witnesses' testimony.

Mr. SHAYS. I thank the gentleman, and recognize Mr. Duncan.

Mr. DUNCAN. Well, thank you very much, Mr. Chairman, for calling this very important hearing.

I don't have a formal written statement or opening statement, but I do want to say that I don't represent the facility at Oak Ridge, TN, but slightly over half of the people who work there live in my district, and so this is a subject of great concern to me and my constituents; and I am particularly interested to know if there are any problems or shortcomings at the facility at Oak Ridge.

But I will just—I have come here mainly to try to learn about this, what the problem is and what the extent of it is; and I thank you for calling this hearing.

Mr. SHAYS. I thank the gentleman for participating and both gentlemen's good work on this committee.

Just a few housekeeping before recognizing our panel. I ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record and that the record remain open for 3 days for that purpose. Without objection, so ordered.

I ask further unanimous consent that all witnesses be permitted to include their written statements in the record, and without objection, so ordered.

I ask unanimous consent that the subcommittee meet in closed session at 2 p.m. today to hear testimony on classified aspects of the issues under discussion today. Without objection so ordered. We will do that at 2 today.

I am going to call on the first panel, recognize them, and then have Mr. Turner take over and conduct this hearing.

Our first panel is comprised of Ms. Robin M. Nazzaro, Director, National Resources and Environment, the U.S. General Accounting Office, accompanied from the same division by James Noel, Assistant Director, and also Jonathan M. Gill, Evaluator.

The second testimony from this panel will be from Glenn Podonsky, Director of Office of Oversight and Performance Assurance, referred to as "OA," from the Department of Energy.

If you would please rise, we will swear you in and we will start the testimony.

[Witnesses sworn.]

Mr. SHAYS. Note for the record, our witnesses have responded in the affirmative. And we will start with Ms. Nazzaro.

Ms. NAZZARO. Thank you, Mr. Chairman.

Mr. SHAYS. Let me just say, we have 5 minutes, but we roll over for another 5 minutes, so you will have, technically, 10 minutes, but we prefer you stop somewhere between the 5 and the 10. It is important that we put your document on the record, so if you need the full 10, feel free to use it.

Ms. NAZZARO. OK. Thank you.

Mr. SHAYS. Thank you.

STATEMENTS OF ROBIN M. NAZZARO, DIRECTOR, NATURAL RESOURCES AND ENVIRONMENT, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY JAMES NOEL, ASSISTANT DIRECTOR, AND JONATHAN M. GILL, EVALUATOR, NATURAL RESOURCES AND ENVIRONMENT; AND GLENN S. PODONSKY, DIRECTOR, OFFICE OF OVERSIGHT AND PERFORMANCE ASSURANCE, U.S. DEPARTMENT OF ENERGY

Ms. NAZZARO. Thank you, Mr. Chairman and members of the subcommittee. I am pleased to be here today to discuss physical security of the nuclear weapons complex at the Department of Energy and the National Nuclear Security Administration within DOE.

Currently, the nuclear complex includes four production sites, three national laboratories that design nuclear weapons and a number of former nuclear weapons sites that contain nuclear weapons materials. To ensure the physical security of the complex, DOE and NNSA rely on their safeguards and security program.

A key component of the DOE's protective strategy is the design basis threat, which identifies the characteristics of the potential threats to DOE. To implement their safeguards and security program, DOE and NNSA rely on contractors to conduct day-to-day security activities subject to DOE and NNSA oversight.

Over the past decade, we and others have raised concern about the adequacy of security at nuclear weapons facilities within the Department and NNSA. In addition, the terrorist attacks of September 11, 2001, highlighted the importance of effective physical security in response to a challenging and well-organized terrorist threat.

In this context, my testimony today focuses on two issues: first, how NNSA manages its safeguards and security program; and second, DOE's response to the terrorist attacks of September 11, 2001.

In summary, Mr. Chairman, we found that NNSA has not been fully effective in managing its safeguards and security program in the following four key areas.

First, NNSA had not fully defined clear roles and responsibilities for its headquarters and site operations. Since its creation in March 2000, NNSA's management structure has been in a state of

flux. As a result, NNSA site office officials said that each office is carrying out oversight activities as it deems appropriate.

Second, as a result of the lack of clarity in NNSA's management structure, NNSA site offices have not been consistent in how they assess contractor safeguards and security activities. Consequently, NNSA cannot be assured that all facilities are subject to the comprehensive annual assessment that DOE policy requires.

Third, once problems are identified, NNSA contractors do not consistently conduct the analysis DOE policy requires in preparing corrective action plans. The corrective actions are developed without fully considering the problems' root causes, the risks posed, or the cost versus benefit of taking corrective action. Thus, potential opportunities to improve physical security at the sites are not maximized.

And last, NNSA site offices have shortfalls in the total number of staff and in the expertise for effectively overseeing contractors. This could make it more difficult for site offices to effectively oversee security activities.

Site officials said that they will fill some vacancies through a virtual organization. However, it will take time to work through some of the difficulties associated with making the transition to this approach.

As a result, NNSA cannot be assured that its contractors are working to a maximum advantage to protect critical facilities and materials from adversaries seeking to inflict damage.

In our May report, we made four recommendations to address these problems, that are designed to improve NNSA's security management and oversight. Since the issuance of our report, NNSA has made progress in addressing the problems we identified, including publishing a Safeguards and Security Functions, Responsibilities, and Authorities Manual and developing and issuing guidance for corrective action plans. Beyond these changes sound safeguards and security management will have to play a key role in helping DOE and NNSA adjust to the post-September 11 security environment.

Before I take the second issue on, do you want me to break? Then, here would be a good place.

Mr. TURNER [presiding]. No. Please continue.

Ms. NAZZARO. Continue? OK.

I would now like to discuss DOE and NNSA response to the terrorist attacks of September 11, 2001. In this regard, we examined three issues: DOE's and NNSA's immediate response to the attacks, DOE's efforts to develop the design basis threat document, and the challenges DOE and NNSA face in meeting the requirements of the new DBT.

DOE and NNSA took immediate steps to improve security in the aftermath of the September 11 terrorist attacks. For example, DOE and NNSA moved to a higher level of security that required, among other things, more vehicle inspections and security patrols. DOE and NNSA also conducted a number of security-related reviews, studies and analysis and increased communication with Federal, State and local officials. While these steps are believed to have improved DOE's and NNSA's security posture, they have been expensive. These steps have required extensive overtime, which has had

a considerable negative effect on DOE's and NNSA's protective force through fatigue, reduced readiness, retention, and reduced training. Furthermore, until fully evaluated, the effectiveness of these measures is uncertain.

Based on the number and capabilities of the terrorists involved in the September 11 attacks, DOE and NNSA officials realized that the then-current DBT, which was issued in 1999 and based on a 1998 Intelligence Community assessment, was obsolete. However, formally recognizing these new threats by updating the DBT has been difficult. DOE's effort to develop and issue a new DBT took almost 2 years; it was issued just last month. The effort to develop a new DBT was slowed by, among other things, disagreements over the size of the potential terrorist group that might attack a DOE or NNSA facility and how much it would cost to meet the new threat.

Implementation of the new DBT will be challenging. Successfully addressing the increased threats will take time and resources as well as sound management, leadership, and new ways of doing business. Currently, DOE does not have a reliable estimate of the cost to fully protect DOE and NNSA facilities against the new DBT. Further, once funds become available, most sites estimate that it will take from 2 to 5 years to fully implement, test, validate, and refine strategies for meeting the new DBT requirements. Meeting these challenges will require DOE and NNSA to provide sustained sound management for their safeguards and security program. Given the materials DOE and NNSA possess, physical security at DOE and NNSA facilities cannot fail.

Mr. Chairman, that concludes my statement. I would be happy to respond to any questions you or the Members may have.

Mr. TURNER. Thank you.

[NOTE.—The GAO report entitled, "Nuclear Security, NNSA Needs to Better Manage Its Safeguards and Security Program," may be found in subcommittee files.]

[The prepared statement of Ms. Nazarro follows:]

United States General Accounting Office

GAO

Testimony

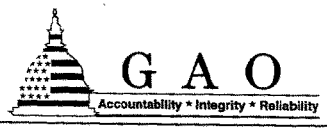
Before the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform

For Release on Delivery
Expected at 9:00 a.m. EDT
June 24, 2003

NUCLEAR SECURITY

DOE Faces Security Challenges in the Post September 11, 2001, Environment

Statement of Robin M. Nazzaro, Director
Natural Resources and Environment Team



)6TNI

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-03-896TNI, a report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

Why GAO Did This Study

The attacks of September 11, 2001, intensified long-standing concerns about the adequacy of safeguards and security at DOE and NNSA that facilities store plutonium and uranium in a variety of forms. These contractor-operated facilities can become targets for such actions as sabotage or theft. The Department of Energy (DOE) and the National Nuclear Security Administration (NNSA)—a separately organized agency within DOE—are responsible for these facilities. GAO reviewed how effectively NNSA manages its safeguards and security program, including how it oversees contractor security operations. GAO also reviewed DOE and NNSA's response to the terrorist attacks of September 11, 2001. In this regard, GAO examined (1) DOE and NNSA's immediate response to September 11, (2) DOE's efforts to develop a new design basis threat, a classified document that identifies the potential size and capabilities of the terrorist forces that DOE and NNSA sites must be prepared to defend against, and (3) the challenges DOE and NNSA face in meeting the requirements of the new design basis threat.

ww.gao.gov/cgi-bin/getrpt?GAO-03-896TNI,

view the full product, including the scope d methodology, click on the link above. more information, contact Robin M. zaro at (202) 512-3841 or zaroR@gao.gov.

June 24, 2003

NUCLEAR SECURITY

DOE Faces Security Challenges in the Post September 11, 2001, Environment

What GAO Found

NNSA has not been fully effective in managing its safeguards and security program. For example, NNSA has not fully defined clear roles and responsibilities for its headquarters and site operations. Without a functional management structure and with ongoing confusion about roles and responsibilities, inconsistencies have emerged among NNSA sites on how they assess contractors' security activities. Consequently, NNSA cannot be assured that all facilities are subject to the comprehensive annual assessments that DOE policy requires. To compound the problems in conducting security assessments, NNSA contractors do not consistently conduct required analyses in preparing corrective action plans. As a result, potential opportunities to improve physical security at the sites are not maximized because corrective actions are developed without fully considering the problems' root causes, risks posed, or cost versus the benefit of taking corrective action. Finally, NNSA has shortfalls at its site offices in the total number of staff and in expertise, which could make it more difficult for site offices to effectively oversee security activities. GAO made recommendations to improve the management of NNSA's safeguards and security program. NNSA has begun to respond to these recommendations.

With respect to DOE and NNSA's response to September 11, the agencies took immediate steps to improve security in the aftermath of the terrorist attacks. For example, DOE and NNSA moved to a higher level of security, which required, among other things, more vehicle inspections and security patrols. While these steps are believed to have improved DOE and NNSA's security posture, they have been expensive and, until fully evaluated, their effectiveness is uncertain.

The number and capabilities of the terrorists involved in the September 11 attacks rendered obsolete DOE's design basis threat, last issued in 1999. However, DOE's effort to develop and issue a new design basis threat took almost 2 years; it was issued in May 2003. This effort was slowed by, among other things, disagreements over the size of the potential terrorist group that might attack a DOE or NNSA facility.

Successfully addressing the increased threats will take time and resources, as well as new ways of doing business, sound management, and leadership. Currently, DOE does not have a reliable estimate of the cost to fully protect DOE and NNSA facilities. The fiscal year 2006 budget will probably be the first to show the full budgetary impact of the new design basis threat. Once funds become available, most sites estimate that it will take from 2 to 5 years to fully implement, test, validate, and refine strategies for meeting the requirements of the new design basis threat.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our work for this Subcommittee on physical security at the Department of Energy (DOE) and the National Nuclear Security Administration (NNSA)—a separately organized agency within DOE.[1] DOE and NNSA recognize that a successful terrorist attack on a facility that contains nuclear weapons or nuclear weapons materials could have devastating consequences for the facility and its surrounding communities.

DOE and NNSA rely on their safeguards and security programs to ensure the physical security of NNSA's nuclear weapons complex. Currently, the complex has four production sites—in Missouri, South Carolina, Tennessee and Texas—and three national laboratories that design nuclear weapons in California and New Mexico. DOE's Office of Environmental Management is responsible for cleaning up former nuclear weapons sites that contain some nuclear weapons materials, including sites in Colorado and Washington State. To implement their safeguards and security programs, NNSA and the Office of Environmental Management rely on contractors that are responsible for conducting day-to-day security activities and adhering to DOE policies. The contractors' activities are subject to DOE/NNSA oversight. NNSA and the Office of Environmental Management have offices—site offices—co-located with each site.

Over the past decade, we and others have raised concerns about the adequacy of security at nuclear weapons facilities within the department and NNSA. For example, we reported to you last month that NNSA needs to better manage its safeguards and security program.[2] Concern over security within the nuclear weapons complex was brought into sharper focus by the September 11, 2001, terrorist attacks. These attacks highlighted the importance of effective physical security in response to a challenging and well-organized terrorist threat.

Following the September 11 terrorist attacks, you asked us to review physical security at DOE and NNSA's most sensitive facilities—those

[1]Physical security is the combination of operational and security equipment, personnel, and procedures used to protect facilities, information, documents, or material against theft, sabotage, diversion, or other criminal acts.

[2]U.S. General Accounting Office, *Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471 (Washington, D.C.: May 30, 2003).

facilities that contain specified quantities of plutonium and highly enriched uranium, which require the Category I level of protection—the highest protection requirement.[3] As agreed with your office, we examined two issues. First, we reviewed how NNSA manages its safeguards and security program. Second, we examined DOE's response to the terrorist attacks of September 11, 2001. In this regard, we examined (1) DOE's and NNSA's immediate response to the attacks; (2) DOE's efforts to develop the design basis threat (DBT), a classified document that identifies the potential size and capabilities of the terrorist forces that DOE and NNSA sites must be prepared to defend against; and (3) the challenges DOE and NNSA face in meeting the requirements of the new DBT.

To carry out our objectives, we reviewed DOE policy and planning documents, including orders, implementation guidance, and reports. We met with officials from DOE and NNSA headquarters and NNSA site offices. We obtained information primarily from DOE's Office of Security, Office of Independent Oversight and Performance Assurance, and Office of Environmental Management; and NNSA's Office of Defense Nuclear Security and NNSA's Nuclear Safeguards and Security Program.[4] We visited NNSA's four production plants and the three design laboratories as well as NNSA's Office of Transportation Safeguards. We also visited four Office of Environmental Management sites that contain Category I special nuclear materials. At each location we met with both federal and contractor officials, observed their physical security operations and obtained and reviewed pertinent supporting documentation, including corrective action plans.

We performed our review from December 2001 through May 2003 in accordance with generally accepted government auditing standards.

[3]Category I special nuclear material that requires Category I level of protection includes plutonium and highly enriched uranium in the form of (1) assembled nuclear weapons and test devices; (2) specified quantities of products containing higher concentrations of plutonium or uranium, such as major nuclear components, and recastable metal; and (3) specified quantities of high-grade materials, such as carbides, oxides, solutions, and nitrates.

[4]We did not include naval reactors in our review because that office is a semiautonomous entity within NNSA with a unique security structure and program.

In summary, we found NNSA has not been fully effective in managing its safeguards and security program in four key areas. As a result, NNSA cannot be assured that its contractors are working to maximum advantage to protect critical facilities and materials from adversaries seeking to inflict damage. Specifically, we found the following:

- NNSA has not fully defined clear roles and responsibilities for its headquarters and site operations.
- Without a stable and effective management structure and with ongoing confusion about roles and responsibilities, inconsistencies have emerged among NNSA site offices on how they assess contractors' security activities. Consequently, NNSA cannot be assured that all facilities are subject to the comprehensive annual assessments that DOE policy requires.
- To compound the problems in conducting security assessments, NNSA contractors do not consistently conduct required analyses in preparing corrective action plans. As a result, potential opportunities to improve physical security at the sites are not maximized because corrective actions are developed without fully considering the problems' root causes, risks posed, or the cost versus benefit of taking corrective action.
- NNSA has shortfalls at its site offices in the total number of staff and in expertise, which could make it more difficult for site offices to effectively oversee security activities.

We made four recommendations designed to improve NNSA's security management and oversight. NNSA concurred with two of our four recommendations and has made progress in addressing the issues we identified, including publishing a *Safeguards and Security Functions, Responsibilities, and Authorities Manual* and developing and issuing guidance for corrective action plans. Beyond these changes, sustained attention and commitment to sound safeguards and security management will be needed as DOE and NNSA adjust to the post-September 11 security environment.

With respect to DOE's and NNSA's response to the September 11 terrorist attacks, we found that the department has taken a number of important steps to respond to the terrorist threat; however, DOE's response has been slow in some vital respects, and DOE and NNSA will need at least several years and an as yet undetermined amount of resources before their sites

are fully prepared to meet the projected threat. Specifically, we found the following:

- DOE and NNSA took immediate steps to improve security in the aftermath of the September 11 terrorist attacks. For example, DOE and NNSA moved to a higher level of security that required, among other things, more vehicle inspections and security patrols. While these steps are believed to have improved DOE and NNSA's security posture, they have been expensive and, until fully evaluated, their effectiveness is uncertain.
- The number and capabilities of the terrorists involved in September 11 attacks rendered obsolete DOE's DBT, last issued in 1999. However, DOE's effort to develop and issue a new DBT took almost 2 years; it issued the new DBT in May 2003. The effort to develop a new DBT was slowed by, among other things, disagreements over the size of the potential terrorist group that might attack a DOE or NNSA facility.
- Successfully addressing the increased threats contained in the new DBT will take time and resources, as well as new ways of doing business, sound management, and leadership. Currently, DOE does not have a reliable estimate of the cost to fully protect DOE and NNSA facilities against the new DBT. DOE and NNSA are developing preliminary cost estimates that could be included in the fiscal year 2005 budget, which is now being formulated. However, the fiscal year 2006 budget will probably be the first to show the full budgetary impact of the new DBT. Once funds become available, most sites estimate that it will take from 2 to 5 years to fully implement, test, validate, and refine strategies for meeting the new DBT requirements. Finally, DOE and NNSA will have to change how they perform physical security through such actions as employing new technologies, consolidating special nuclear materials, and closing unneeded facilities.

Background

From the beginning of the Manhattan Project in the 1940s, a primary mission of DOE and its predecessor organizations has been to design, test, and build the nation's nuclear weapons. To accomplish this mission, DOE constructed a vast nuclear weapons complex throughout the United States. Much of this complex was devoted to the production and fabrication of weapons components made from two special nuclear materials—plutonium and highly enriched uranium.

The end of the Cold War changed the department's focus from building new weapons to extending the lives of existing weapons, disposing of surplus nuclear material, and cleaning up no longer needed weapons sites.

NNSA is responsible for extending the lives of existing weapons in the stockpile and for ultimately disposing of surplus nuclear material, while the Office of Environmental Management is responsible for cleaning up former nuclear weapons sites. Contractors, who are responsible for protecting classified information, nuclear materials, nuclear weapons, and nuclear weapons components, operate both NNSA and Office of Environmental Management sites.[5,6]

Besides NNSA and the Office of Environmental Management, DOE has two other important security organizations. DOE's Office of Security develops and promulgates orders and policies, such as the DBT, to guide DOE and NNSA's safeguards and security programs. DOE's Office of Independent Oversight and Performance Assurance supports DOE and NNSA by, among other things, independently evaluating the effectiveness of contractors' performance in safeguards and security. It also performs follow-up reviews to ensure that contractors have taken effective corrective actions and appropriately addressed weaknesses in safeguards and security.

A key component of DOE's protective strategy is the DBT, a classified document that identifies the characteristics of the potential threats to DOE assets. The DBT considers a variety of threats in addition to terrorists: criminals, psychotics, disgruntled employees, violent activists, insiders, and spies. The terrorist threat is generally the most demanding threat contained in the DBT. The DBT has traditionally been informed and shaped by classified multiagency intelligence assessments of potential terrorists threats. The basis for DOE's 2003 DBT is an intelligence community assessment entitled the *Postulated Threat to U.S. Nuclear Weapons Facilities and other Selected Strategic Facilities* (henceforth referred to as the Postulated Threat).

DOE counters the terrorist threat specified in the DBT with a multifaceted protective system. While specific measures vary from site to site, all protective systems at DOE's and NNSA's most sensitive sites employ a defense-in-depth concept that includes

[5]Responsibility for the Idaho National Environmental Engineering Laboratory has been transferred to DOE's Nuclear Energy Program.

[6]An exception is the Office of Transportation Safeguards, whose protective forces are Special Federal Agents.

- a variety of integrated alarms and sensors capable of detecting intruders;
- physical barriers, such as fences and anti-vehicle obstacles;
- numerous access control points, such as turnstiles, badge readers, vehicle inspection stations, special nuclear material detectors, and metal detectors;
- operational security procedures, such as a "two person" rule that prevents only one person from having access to special nuclear material;
- hardened facilities and/or vaults; and
- a heavily armed paramilitary protective force equipped with such items as automatic weapons, night vision equipment, body armor, and chemical protective gear.

Depending on the material, protective systems at DOE and NNSA Category I sites are designed to accomplish the following objectives in response to the terrorist threat.

- **Denial of access.** For some potential terrorist scenarios, DOE employs a protection strategy that requires the engagement and neutralization of an adversary before the adversary can acquire hands-on access to the assets.
- **Denial of task.** For assets that might present terrorists with opportunities to steal a nuclear weapon or nuclear test device, DOE requires the prevention and/or neutralization of the adversary before the adversary can complete a specific task.
- **Containment with recapture.** In scenarios where the theft of nuclear material (instead of a nuclear weapon) is the likely terrorist objective, DOE requires that adversaries not be allowed to escape the facility and that DOE protective forces recapture the material as soon as possible. This objective requires the use of specially trained and well-equipped special response teams.

The effectiveness of the protective system is formally and regularly examined through a vulnerability assessment. A vulnerability assessment is a systematic evaluation process in which qualitative and quantitative techniques are applied to detect vulnerabilities and arrive at effective protection of specific targets, such as special nuclear material. To conduct this assessment, DOE uses, among other things, subject matter experts, such as U.S. Special Forces; computer modeling to simulate attacks; and

force-on-force performance testing, in which the site's protective forces undergo simulated attacks by an adversary team.

The results of these assessments are documented at each site in a classified document known as the Site Safeguards and Security Plan. In addition to identifying known vulnerabilities and risks and protection strategies for the site, the Site Safeguards and Security Plan formally acknowledges how much risk the contractor and DOE are willing to accept. Specifically, for more than a decade, DOE has employed a risk management approach that seeks to direct resources to its most critical assets—in this case specified quantities of Category I special nuclear material—and mitigate the risks to these assets to an acceptable level. DOE strives to keep its most critical assets at a low risk level and may insist on immediate compensatory measures should a significant vulnerability develop. Compensatory measures could include such things as deploying additional protective forces.

Through a variety of complementary measures, DOE ensures that its safeguards and security policies are being complied with and are performing as intended. Contractors perform regular self-assessments and are encouraged to uncover any problems themselves. In addition to routine oversight, DOE and NNSA site offices are required by DOE Orders to conduct comprehensive annual surveys of contractors' operations for safeguards and security. These surveys, which can draw upon subject matter experts throughout the complex, generally take about 2 weeks to conduct and cover such areas as program management, protection program operations, information security, nuclear materials control and accountability, and personnel security. The survey team assigns ratings of satisfactory, marginal, or unsatisfactory. Currently, most of the DOE and NNSA facilities that we examined have been rated satisfactory in most areas. All deficiencies (findings) identified during a survey require the contractors to take corrective action. DOE's Office of Independent Oversight and Performance Assurance provides yet another check through its comprehensive inspection program. This office performs such inspections roughly every 18 months at each DOE and NNSA site that has Category I special nuclear material.

NNSA Needs to Better Manage Its Safeguards and Security Program

As we reported to you on May 30, 2003, NNSA has not been fully effective in managing its safeguards and security program in four key areas, and therefore it cannot be assured that its contractors are working to maximum advantage to protect critical facilities and materials from individuals seeking to inflict damage. The four key areas are the following:

- **Defining clear roles and responsibilities.** Since its creation in March 2000, NNSA's management structure has been in a state of flux. In December 2002, NNSA issued what it considers final directives for reorganizing headquarters and site offices; however, NNSA expects it will take until at least September 2004 to fully implement its new management structure. This still-developing management structure has led to confusion about the safeguards and security roles and responsibilities of headquarters and site offices. For example, at the time of our review, NNSA headquarters could not provide details on how it intends to (1) monitor the NNSA site offices' performance with respect to safeguards and security or (2) address deficiencies. At the end of May 2003, however, NNSA released a *Safeguards and Security Functions, Responsibilities and Authorities Manual.* This manual, which NNSA itself recognizes as crucial, is intended to set out roles and responsibilities clearly.

- **Assessing sites' security activities.** Without a functional management structure and with ongoing confusion about roles and responsibilities, inconsistencies have emerged among the NNSA sites on how to conduct key aspects of safeguards and security assessment activities. In particular, three out of the seven NNSA site offices use the traditional survey approach, as required by DOE policy, to oversee security activities, while four have discontinued surveys and instead rely on surveillance activities. The distinction between these two activities is important: A survey provides a comprehensive annual review, by a team of experts from throughout NNSA, of contractor safeguards and security and generally takes about 2 weeks. In contrast, surveillance relies on a single or small number of NNSA site officials to oversee one or more aspects of a contractor's safeguards and security activities throughout the year. However, officials from DOE's Office of Security—which developed the policy for conducting surveys—believe the surveillance model does not comply with the DOE order because it does not provide a comprehensive overview. Furthermore, officials from DOE's Office of Independent Oversight and Performance Assurance and NNSA headquarters have expressed concern about the site offices' ability to conduct surveillance because of shortfalls in available expertise. The four site offices have been able to operate using only surveillance activities because, during the reorganization of the management structure, NNSA has not issued guidance on complying with DOE policy for conducting surveys.

- **Overseeing contractors' corrective actions.** NNSA contractors do not consistently conduct the analyses DOE policy requires in preparing corrective action plans, which compounds the problems of ensuring physical security. Inconsistency occurs because the NNSA site officials do not have implementation guidance from headquarters on how to address corrective actions. Of the 43 corrective action plans we reviewed for 1999 through 2002, less than half showed that the contractor had performed the required root cause analysis. Furthermore, less than 25 percent demonstrated that the contractor had performed a required risk assessment or cost-benefit analysis. As a result, potential opportunities to improve physical security at the sites were not maximized because corrective actions were developed without fully considering the problems' root causes, risks posed, or cost versus benefit of taking corrective action. However, at the seven sites we visited in 2002, the site offices and contractors are making some progress in establishing formal processes for root cause and other analyses. Nevertheless, inconsistencies remain regarding the approaches used to complete these analyses. For example, some site processes specify that root cause analyses will be conducted for all corrective action plans, while other sites consider the completion of these analyses optional. NNSA did, however, recently issue guidance to its sites regarding compliance with DOE Orders on corrective actions.

- **Allocating staff.** NNSA has shortfalls at its site offices in the total number of staff and in areas of expertise, which could make it more difficult for the site offices to oversee safeguards and security effectively and to ensure that the agency fully knows security conditions at its sites. According to officials at five of the seven site offices we visited, they have, or expect to have, an average of 2 to 6 vacancies per site for overseeing contractors' safeguards and security; typically, each site expects to have 10 to 14 security-related positions within the next 2 years. The vacancies occur, in part, because staff are reluctant to move to locations they view as less desirable and because NNSA has frozen hiring in response to budget constraints. Some of these vacancies are for specialists in particular subject areas, such as Industrial Security Systems—a key specialty needed for conducting physical security inspections. The lack of expertise and staff could be further complicated for some sites by NNSA's realignment plan. Under this plan, NNSA expects to streamline federal oversight of contractors and reduce headquarters and field staff by 20 percent by the end of fiscal year 2004. Site officials said that they will fill some vacancies through a virtual organization in which experts at other locations will assist with certain components of the surveillance activities. However, it will take time to work through some of the difficulties associated with making the transition to this approach.

DOE and NNSA's Response to the Terrorist Attacks of September 11, 2001

I would like now to discuss DOE and NNSA's response to the terrorist attacks of September 11, 2001. I will cover DOE's and NNSA's immediate response to the attacks; DOE's efforts to develop a new DBT that DOE and NNSA sites must be prepared to defend against; and the challenges DOE and NNSA face in meeting the requirements of the new DBT.

DOE and NNSA Improved Security after September 11, 2001, but Have Not Fully Tested These Improvements

DOE and NNSA took immediate steps to improve physical security in the aftermath of the September 11, 2001, terrorist attacks. These steps included the following:

- **Raised the Level of Security Readiness.** DOE's most visible effort involved moving to higher levels of security readiness, as outlined by DOE Notice 473.6. This notice specifies DOE Security Condition, or SECON, levels and the corresponding security measures that have to be implemented.[7] On September 11, 2001, within a matter of hours, DOE and NNSA sites went from their then-normal SECON level 4—terrorist threat level low—to SECON level 2—terrorist threat level high. Sites were required to implement nearly 30 additional measures, such as increasing vehicle inspections and badge checks; increasing stand-off distances between public and sensitive areas; activating and manning emergency operations centers on a continuous basis; and more heavily arming and increasing the number of protective forces on duty. Sites maintained SECON level 2 through October 2001 before dropping to an enhanced SECON level 3. The sites have returned to SECON level 2 several times since September 11 2001, most recently in May 2003, when the national threat warning systems was elevated to Orange Alert. The new baseline for security at DOE and NNSA facilities is generally assumed to be at an enhanced SECON level 3. This level is still substantially greater than DOE's pre-September 11, 2001 security posture.

- **Enhanced Protective Force Responses.** On October 3, 2001, the Secretary of Energy issued a classified directive that ordered more robust protective force responses and increased levels of performance testing for the protection of certain special nuclear material at DOE's and NNSA's most critical facilities.

[7]SECON levels are pegged to the national threat level issued by the Department of Homeland Security. For example, a national level of ORANGE equates to SECON level 2 for DOE facilities.

- **Conducted Security Reviews, Studies and Analyses.** DOE and NNSA also conducted a number of security-related reviews, studies, and analyses. For example, within days after the terrorist attacks, DOE and NNSA officials conducted a classified assessment of their facilities' vulnerabilities to an attack such as the one on September 11. This assessment came to be known as the *72 Hour Review*. In addition, NNSA organized a 90-day Combating Terrorism Task Force, composed of 12 federal and contractor employee teams that looked at a number of security areas. One team, the site-by-site security review and vulnerability assessment group, identified over 80 prioritized security improvement projects, totaling more than $2 billion, that could be completed within 5 to 6 years. These projects ranged from hiring additional protective forces to consolidating special nuclear material.

- **Increased Liaison with Federal, State, and Local Authorities:** Before the September 11 terrorist attacks, DOE and NNSA headquarters offices and sites maintained a variety of relationships, memoranda of understanding, and other formal and informal communications with organizations such as the Federal Aviation Administration, Federal Bureau of Investigation, and state and local law enforcement and emergency management agencies. After the terrorist attacks, DOE and NNSA officials increased their communication with these organizations and established direct links through sites' emergency operations centers. Because of the potential threat of aircraft attacks created by the September 11 attacks, sites worked closely with the Federal Aviation Administration and the U.S. military.

While these steps are believed to have generally improved security, they have been expensive and, until fully tested using DOE's vulnerability analysis approach, their effectiveness is uncertain. With respect to improved security, implementation of SECON levels 2 and 3 has, for example, increased the visible deterrence at DOE and NNSA sites by placing more guards around the sites. Studies and analyses, such as the *72 Hour Review*, have also resulted in different and less vulnerable storage strategies for some special nuclear material. DOE and NNSA have hired additional protective forces and are training them. Finally, some long-recognized security enhancement projects have received more funding, such as the construction of a new highly enriched uranium materials facility at the Y-12 Plant, and the removal of some of the Los Alamos National Laboratory's most sensitive materials and equipment to a more modern facility at the Nevada Test Site have been accelerated.

At the same time, it has been expensive to implement the increased SECON measures. DOE and NNSA sites estimate that it costs each site

from $18,000 to nearly $200,000 per week in unplanned expenditures to implement the required SECON level 2 and 3 measures. Most of these expenses result from overtime pay to protective forces.

However, the costs of the higher SECON levels can be measured in more than just budget dollars. For example, a recent DOE Inspector's General report found that the large amounts of overtime needed to meet the higher SECON requirements have resulted in fatigue, reduced readiness, retention problems, reduced training, and fewer force-on-force performance tests for the protective forces.[8] In addition, the increased operational costs associated with the higher SECON levels can hinder or preclude sites from making investments that could improve their security over the long term. For example, one site delayed purchasing equipment for its protective force that would address a known vulnerability because of the high costs of SECON implementation. Finally, implementation of the protective force response plans outlined in the Secretary's October 3, 2001, directive was sharply limited by the lack of available funding, with some sites estimating it would take from about $30 million to over $200 million to implement the directive completely. Moreover, the performance testing requirements of this directive were generally not conducted because of the already large amounts of protective force overtime required by the higher SECON levels. The new DBT, however, has replaced this directive.

Other than deterrence, the role of the higher SECON levels in improving DOE and NNSA physical security is uncertain. Some aspects of the SECON measures, such as vehicle inspection checkpoints have undergone some limited testing of their effectiveness. However, the higher SECON level measures in place at most sites have not been assessed using the vulnerability assessment tools, such as computer modeling and full-scale force-on-force exercises, that play such a key role in developing protective strategies for DOE and NNSA sites.

Finally, while liaison with other agencies is important, DOE and NNSA site officials anticipate that terrorist attacks on their facilities will be short and violent affairs and will be over before any external responders can arrive on site. In addition, because some DOE and NNSA sites are close to airports and/or major flight routes, they may receive little warning of

[8] *Audit Report: Management of the Department's Protective Forces*, DOE/IG-0602, Department of Energy Office of the Inspector General, June 2003.

aircraft attacks and U.S. military aircraft may have little opportunity to intercept these attacks.

Development of a New DBT Was Difficult, but Resulted in a Higher Threat Level

In the immediate aftermath of September 11, 2001, DOE and NNSA officials realized that the then current DBT, issued in 1999 and based on a 1998 intelligence community assessment, was largely obsolete. The terrorist attacks suggested larger groups of adversaries, larger vehicle bombs, and broader terrorist aspirations to cause mass casualties and panic than were envisioned in the 1999 DOE DBT. However, formally recognizing these new threats by updating the DBT has proven difficult.

The traditional basis for the DBT has been a study, known as the Postulated Threat, conducted by the U.S. intelligence community and agency security organizations, principally the Department of Defense's (DOD) Defense Intelligence Agency. However, the new Postulated Threat was completed about 9 months behind its original schedule and not finally released until January 2003. According to DOE and DOD officials, this delay was the result of other post-September 11, 2001, demands placed on the intelligence community as well as sharp debates among the organizations involved with developing the Postulated Threat over the size and capabilities of future terrorist threats and the resources needed to meet these projected threats.

Given the delay associated with the development of the Postulated Threat, DOE, on its own, developed a number of draft threat statements that culminated in the final May 20, 2003, DBT. These included the following:

- **December 2001—Interim Joint Threat Policy Statement.** DOE and DOD worked on this joint draft document but abandoned this effort later in 2002.
- **January 2002—Interim Implementing Guidance.** DOE's Security Office issued this guidance so that DOE and NNSA programs could begin to plan for eventual increases in the DBT.
- **May 2002—Draft DBT.** DOE produced its official draft DBT. This was labeled an interim product pending the release of the Postulated Threat.
- **August 2002—2nd Draft DBT.**
- **December 2002—3rd Draft DBT.**

- **April 2003—4th Draft DBT.**
- **May 2003—Final DBT.**

DOE's Security Office distributed the drafts to DOE and NNSA program and site offices and invited them to provide comments. DOE's Security Office considered these comments and often incorporated them into the next version of the DBT. DOE's Security Office also continued to coordinate with the other federal organizations that have similar assets, chiefly DOD and the Nuclear Regulatory Commission.

During the development of DOE's DBT, debates, similar to those that occurred during the development of the Postulated Threat, emerged in DOE and NNSA over the size of the future threat and how much it would cost to meet the new threat. DOE and NNSA officials from all levels told us that concern over resources played a large role in developing the 2003 DBT, with some officials calling the DBT the "funding basis threat," or the maximum threat the department could afford. This tension between threat size and resources is not a new development. According to a DOE analysis of the development of prior DBTs, political and budgetary pressures and the apparent desire to reduce protective force manpower requirements appear to have played a significant role in determining the adversary numbers contained in prior DBTs.

Reflecting the post-September 11, 2001, environment, the 2003 DBT is a substantially different and more demanding document than previous DBTs. Key differences from the 1999 DBT include the following:

- **Increased adversary threat levels.** The 2003 DBT increases the terrorist threat levels for the theft of the department's highest value assets—special nuclear material—although not in a uniform way. The 1999 DBT required DOE and NNSA sites to protect against only one terrorist threat level. Under the 2003 DBT, however, the theft of a nuclear weapon or test assembly is judged to be more attractive to terrorists, and sites that have these assets are required to defend against a substantially higher number of adversaries than are other DOE and NNSA sites that possess other forms of Category I quantities of special nuclear material. For example, the Pantex Plant, which, among other things, assembles and disassembles nuclear weapons, is required to defend to a higher level than sites such Los Alamos or Y-12, both of which fabricate nuclear weapons components. DOE calls this a graded threat approach.

- **Specific protection strategies.** In line with the graded threat approach and depending on the type of materials they possess and the likely mission of the terrorist group, sites are now required to implement specific protection strategies, such as denial of access, denial of task, or containment with recapture for their most sensitive facilities and assets.

- **Wider range of terrorist objectives.** The 2003 DBT recognizes a wider range of terrorist objectives, particularly in the area of radiological, chemical, and biological sabotage. The 2003 DBT requires the development of protection strategies for a range of facilities, such as some radioactive waste storage areas, that were not covered under the previous DBT.

- **Increased Complexity.** With a graded approach and broader coverage, the new DBT is a more complex document than its predecessor. For example, the 1999 DBT was 9 pages long, while the 2003 DBT is 48 pages long.

During the 21 months it took to develop the DBT policy, DOE and NNSA sites still officially followed the 1999 DBT, although their protective posture was augmented by implementing SECON level 2 and 3 measures. While DOE sites under the Office of Environmental Management continued to conduct vulnerability assessments and develop Site Safeguards and Security Plans based on the 1999 DBT, NNSA largely suspended the development of Site Safeguards and Security Plans pending the issuance of the new DBT. During this period, however, NNSA did embark on a new vulnerability assessment process, called Iterative Site Analysis, at four sites and its Office of Transportation Safeguards. The Iterative Site Analyses were analytical, tabletop exercises that addressed a spectrum of potential threats, both within and beyond the threat contained in the 1999 DBT. Iterative Site Analyses were conducted by independent and highly skilled security professionals from across the government and private sector. Most NNSA sites agreed that the Iterative Site Analysis exercises were valuable, and some sites believe that it gave them a head start in meeting the requirements of the new DBT. The Office of Environmental Management is testing this methodology at one of its sites this summer. DOE's Office of Independent Oversight and Performance Assurance continued its inspections; however, it initially reduced the amount of force-on-force performance testing it conducted because of the high levels of protective force overtime caused by implementation of SECON level 2 and 3 measures. This Office also planned to begin performance testing at levels beyond the 1999 DBT, but had done so at only one site before the 2003 DBT was issued.

Implementation of the 2003 DBT Will Be Challenging

Successfully addressing the increased threats contained in the 2003 DBT will take time and resources, as well as new ways of doing business, sound management, and leadership. Currently, the department does not have a reliable estimate for the total cost of fully protecting DOE and NNSA facilities against the 2003 DBT. While DOE and NNSA officials expect new resource requirements to vary widely among the sites, neither the current fiscal year 2003 nor the planned fiscal year 2004 budget includes funds for implementing the 2003 DBT. DOE and NNSA are currently developing preliminary cost estimates that could be included in the fiscal year 2005 budget, which is now being formulated; however, the fiscal year 2006 budget will probably be the first to show the full budgetary impact of the new DBT. DOE and NNSA officials suggest that in order to take earlier action, they may pursue additional security funding through reprogramming and/or supplemental appropriations.

Once funds become available, most sites estimate that it will take from 2 to 5 years to fully implement, test, validate, and refine strategies for meeting the new DBT requirements. Some sites, particularly those that benefited from the Iterative Site Analysis, may be able to move more quickly, and all sites will continue to place priority on improving the protection of special nuclear material.

DOE and NNSA officials also recognize that they will have to change how they perform the physical security mission. A DOE 1999 report and a 2002 NNSA report, this time reinforced by the September 11 attacks, called for changes in the way the department approaches physical security.[9] These changes will be even more important now that the 2003 DBT has been issued. DOE and NNSA are seeking to

- develop and employ new technologies;
- accelerate the design and construction of new facilities;
- better utilize existing facilities;
- purchase adjacent public lands, close public roads and/or build bypass roads around key facilities to restrict public access; and

[9] *A Context and Strategy for Action: A Synthesis of the Special Security Review for DOE Executive Management*, December 1998; *A Security Architecture for NNSA: A Proposed Framework for Planning and Managing Security*, May 23, 2002.

- consolidate special nuclear material and close unneeded facilities.

DOE and NNSA have taken some steps in these directions, but will have to accomplish more to meet the post-September 11, 2001, security challenges. For example:

- **Developing and Employing New Technologies.** Security at many DOE and NNSA sites is a manpower-intensive activity. Adding additional protective forces to facilities is a flexible, effective, but ultimately expensive way of providing additional security. DOE's Security Office has funded a technology development and assessment program and NNSA is initiating its own program in fiscal year 2004; however, the amount of funds devoted to these activities has been limited. The use of technology in areas such as communications, weaponry, intrusion detection, and better computer modeling offers the promise of more effective security at, ultimately, lower costs.

- **Accelerating the Design and Construction of New and Better Protected Facilities.** It is difficult, expensive, and sometimes impossible to retrofit existing facilities to meet more demanding physical security requirements, such as those identified in the 2003 DBT. It is far better to make security an integral part of the design of a new facility. For example, DOE estimated that a new facility built to centrally store special nuclear material would have very steep up-front costs of $2.5 to $4 billion, but would pay for itself in 4 years because of savings from reducing the number protective forces and reducing costs for safeguards and security maintenance. While DOE is not currently planning for such a facility, it is now designing or constructing a number of new facilities at several sites that will be better protected than existing facilities, although their level of protection against the 2003 DBT is uncertain. One of these new facilities, the highly enriched uranium materials facility at the Y-12 plant, may be completed as early as fiscal year 2008.

- **Better Utilization of Existing Facilities.** DOE and NNSA had made some progress in this area, even before September 11, 2001. For example, the old K Area Reactor at the Savannah River Site, a massively constructed building already outfitted with physical security systems, was converted to an interim plutonium storage facility and is currently accepting shipments of plutonium from Rocky Flats. In addition, planning is underway to move sensitive equipment and materials from Technical Area –18 at Los Alamos to the more modern Device Assembly Facility at the Nevada Test Site. However, this move is expected to cost $130 million and not be completed until fiscal year 2009.

- **Purchasing Adjacent Public Lands, Closing Public Roads and/or Building Bypass Roads Around Key Facilities to Restrict Public Access.** A number of sites are bisected or adjacent to public roads and areas. Public access to these roads and areas has been restricted since September 11, 2001, and more permanent measures are being implemented or studied at sites such as Pantex, Lawrence Livermore, Los Alamos, and Y-12.

- **Closing Unneeded Facilities and Consolidating Special Nuclear Material.** DOE's Office of Environmental Management has long had the goal of closing unneeded facilities and consolidating special nuclear material. The Office of Environmental Management has recently proposed accelerating the deadline from 2016 to 2006 for moving Category I special nuclear material from Hanford and Rocky Flats to its Savannah River Site. At Savannah River, materials will ultimately be disposed of or transferred to other program offices, such as NNSA and DOE's Nuclear Energy Program. The Office of Environmental Management expects that all Category I special nuclear material will be removed from Rocky Flats by the end of the summer, 2003.

In closing, it will be a challenge for DOE and NNSA to deal with the post-September 11 security threats. DOE and NNSA have been providing physical security for over 50 years; however, given the materials and assets they possess, physical security at DOE and NNSA facilities cannot afford to fail, even once.

Meeting these challenges will require DOE and NNSA to provide sustained, sound management for their safeguards and security programs. This is particularly true for NNSA because it is the enduring steward for the nation's special nuclear material and is responsible for ensuring that the nation's nuclear weapons are safe and reliable.

Equally important DOE and NNSA must exercise strong, sustained, and high-level leadership in providing for safeguards and security. Security officials often told us that the department has a history of alternating periods of inattention and attention to security. In the post September 11, 2001, environment, the stakes are too high to allow such lapses in the future.

Mr. Chairman, this concludes my testimony. I would be happy to respond to any questions you or Members of the Subcommittee may have.

GAO Contact and Staff Acknowledgments

For further information on this testimony, please contact Robin M. Nazzaro at (202) 512-3841. James Noel, Jonathan Gill, Chris Pacheco, Andrea Miller, Chris Abraham, and Jill Berman also made key contributions to this testimony.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Mr. TURNER. Mr. Noel. I am sorry. Mr. Podonsky.

Mr. PODONSKY. Thank you, Mr. Chairman, for inviting me to testify today.

My Office of Independent Oversight and Performance Assurance is responsible for evaluating the Department's environment, safety, and health, safeguarding the security and cyber security programs at the Department. We report directly to the Secretary of Energy and have no responsibilities for either managing DOE sites or developing policy. Consequently, we perform assessments independent of the programs and provide unbiased information to the Secretary, the NNSA Administrator and other DOE line managers.

My testimony today will focus on the current status of security programs at nuclear weapons production sites and the national weapons laboratories.

It is important to note that some of the current problems in the DOE security program are driven by events that occurred in the mid-90's when budgets for security were cut significantly. These cuts resulted in reductions in protective forces and decisions not to upgrade or replace security hardware. In the 1998 timeframe, independent oversight reviews, and other external assessments revealed that the security cuts had gone too far at some sites; protection effectiveness was not where it needed to be. At DOE's direction, sites began rebuilding their protection programs.

The tragic events of September 11 happened at a time when DOE was still rebuilding its protection programs. Since then, DOE has increased security through a number of measures and has reassessed the design basis threat. However, these represent only the first steps in enhancing DOE security.

Historically, many roles and responsibilities for security have been unclear in some areas and too fragmented for effective operation in others. Secretary Abraham and Ambassador Brooks are addressing the overall management structure for security, but much remains to be done before DOE has a coherent management structure in place to support an effective corporate approach to security.

Our assessment of the current security posture is based on inspections we have conducted during the past 2 years, which include most major NNSA sites and laboratories. Our inspections include extensive performance testing. For example, we have been conducting much more aggressive large-scale force-on-force performance tests of physical security using our own adversary team for years. The September 11 events prompted us to redouble our efforts. Since then we have substantially increased the number of tests we perform and strengthened our adversaries team by adding real-world experts and rigorous training.

At the direction of Secretary Abraham, we are initiating a DOE-wide review of protective force operations to assess the current effectiveness of post-September 11 enhancements. Our inspections and performance tests have documented some positive aspects, as well as a number of weaknesses, some of which are long-standing and require substantially more attention.

On the positive side, many improvements have resulted from the increased security measures put in place following September 11. DOE sites have hired more protective force personnel and in-

creased the number of protective force members on duty at any given time. They have added additional barriers and hardened fighting positions. Classified cyber operations have also been made more secure.

Additionally, Secretary Abraham personally directed that the design basis threat be further strengthened after it was submitted for his review. The final design basis threat, which was issued May 20, provides the basis for establishing and assessing protection effectiveness at DOE sites.

Notwithstanding these positive aspects, our inspections have also documented a number of weaknesses. The recent hire of additional protective force personnel has been responsive to the heightened security levels. However, DOE sites continue to rely on the use of overtime until new hires are cleared and trained to perform their duties. As a result, protective force personnel testing and training have been reduced or deferred because existing manpower is stretched to the limit.

DOE sites have primarily responded to the need to enhance security by using manpower-intensive measures. More effective solutions can be gained by enhancing the integration of manpower and technology through increased use of barriers and force multipliers, consolidating security assets, improving manpower deployment to protect vital assets, and making greater use of performance tests.

It is clear that every site has increased its level of protection in response to the September 11 attacks. However, few of these enhanced protection schemes have been fully performance-tested or formally evaluated.

Unclassified cyber security continues to be a challenge for many sites. There are recurring deficiencies regarding controls of foreign nationals on DOE computer systems. Additionally, some sites have not fully recognized or addressed the risk associated with the proliferation of wireless computer technology. Weakness in feedback, in improving the process and clarity of security roles and responsibilities are long-standing concerns within both the DOE line and contractor organizations. Progress in these areas has been inconsistent and sporadic.

The NNSA reorganization places increased responsibility onsite offices. However, at this time, not all sites have the staffing and expertise necessary to fully and effectively discharge their security oversight responsibility. The Secretary, Deputy Secretary and NNSA Administrator have placed significant emphasis on reorganizing the management structure to clarify responsibilities and increase accountability. They have demonstrated personal involvement in enhancing security after September 11 and in response to the very recent security lapses. The current efforts are promising, but need significant continued attention and evaluation to ensure that the intended improvements are realized at the field level.

In closing, the Department is making some progress, but much more work is needed to upgrade and vigorously test site programs to meet the new design basis threat, to crystallize security-related roles and responsibilities throughout the Department, and to apply program and performance feedback in continuously improving our overall security posture. The strong and aggressive focus of the Secretary and the NNSA Administrator must be sustained in order

to satisfy the increasingly complex and continually changing security challenges that face the DOE and our Nation.

Thank you.

Mr. TURNER. Thank you.

[The prepared statement of Mr. Podonsky follows:]

UNCLASSIFIED TESTIMONY
GLENN S. PODONSKY
DIRECTOR
OFFICE OF INDEPENDENT OVERSIGHT AND PERFORMANCE ASSURANCE
U.S. DEPARTMENT OF ENERGY
BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS
COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

June 24, 2003

Introductory Remarks
Thank you, Mr. Chairman, for inviting me to testify today. My office – the Office of Independent Oversight and Performance Assurance – is responsible for evaluating the Department's environment, safety, and health; emergency management; cyber security; and safeguards and security programs. We report directly to the Secretary of Energy and have no responsibilities for managing DOE sites or for developing policy. As a result, we are able to perform independent assessments of the effectiveness of programs and provide unbiased information to the Secretary and DOE line managers.

In the area of security programs at nuclear weapons complex facilities, we perform regular inspections of all DOE sites that have special nuclear materials and classified information related to the nuclear weapons programs, including all NNSA sites. We inspect the sites against DOE requirements, including the DOE design basis threat policy. However, we also examine the effectiveness of DOE policy in providing protection for our national assets and from time to time identify opportunities to improve DOE security policies.

The focus of my testimony today will be on the current status of security programs at the nuclear weapons production facilities and the national laboratories that design nuclear weapons. However, a brief review of the evolution of the security program is necessary to place the proper context on current security programs. DOE first established an Independent Oversight program twenty years ago. At that time, DOE security systems were in very bad shape. Some nuclear facilities did not even have functional intrusion alarm systems. Protective forces were understaffed, poorly trained, poorly conditioned, and poorly managed. DOE sites were not able to defeat the threat in many cases, as evidenced by numerous performance tests conducted by Independent Oversight and other groups. Recognizing the inadequate levels of security, during the late 1980s, DOE invested close to a billion dollars in improved physical security systems and protective force training. These investments resulted in dramatic improvements in security. However, at several sites, the alarm systems installed 15 years ago are at or near the end of their expected life, and now require extensive maintenance and/or replacement.

During the mid-1990s, budgets for security were reduced significantly at most DOE sites from the high levels required to improve our security posture to a steady-state level, and as part of a widespread effort to more efficiently manage overhead costs. These reductions were a result of

the end of the Cold War and an increased focus on environment, safety and health programs. The impact of these changes caused significant reductions in protective forces and decisions not to upgrade or replace security hardware. In most cases, sites compensated for the smaller number of protective force personnel by consolidating nuclear materials into fewer areas and other means, such as more use of electronic access control systems to replace guards. In the 1998 timeframe, Independent Oversight reviews and other external assessments revealed that the security reductions at a number of sites had gone too far—the protection effectiveness was not where it needed to be. However, we are not implying that sites had reached the poor levels of security that were evident in the early 1980s. However, the cost cutting measures went too far and the protection effectiveness was not where it needed to be. At DOE's direction, sites began to rebuild their protection programs including additional personnel, better equipment, and increased training. However, the ramifications of the reductions in the security budgets took several years to overcome, considering the time needed to obtain budget approval for new protective personnel, obtain security clearances, get personnel trained, and test and fine tune response plans.

Another important trend that has impacted security is the proliferation of computers, electronic data files, and the Internet. DOE experienced a number of security lapses in the late 1990s involving classified or sensitive information, such as the well-publicized loss of the hard drive at the Los Alamos National Laboratory. Many of these security lapses were partially attributable to the fact that DOE policies and practices in the cyber security arena did not always keep pace with changing technology. Independent Oversight has made cyber security a major focus area for over five years now, and DOE took a number of important steps to enhance policies and practices in the protection of information.

The tragic events of September 11, 2001 happened at a time when DOE was still rebuilding its protection programs. DOE, like everyone else, took 9-11 as a wake up call. Since then, DOE has increased security through a number of measures, and has additionally reassessed the design basis threat. However, these represent only the immediate first steps in enhancing DOE security. Historically, roles and responsibilities for security have been unclear in some areas and too fragmented for effective operation in others. Secretary Abraham personally directed that the DOE design basis threat be strengthened. The design basis threat, which was issued May 20th, provides the basis for establishing and assessing protection effectiveness at DOE sites. Secretary Abraham and Ambassador Brooks are addressing the overall management structure for security, but much remains to be done before DOE has a coherent management structure in place to support an effective corporate approach to security.

Independent Oversight Approach and Recent Actions

Our assessment of the current status is based on the inspections that we have performed in the past two years. Since 9-11, Independent Oversight has conducted reviews at all major NNSA production sites and weapons laboratories with the exception of Sandia National Laboratories and the Nevada Test Site. We are currently performing a limited scope review at Sandia National Laboratories and will conduct a comprehensive inspection this fall. We plan to inspect the Nevada Test Site in the near future, after we complete a DOE-wide review of protective forces, which was directed by Secretary Abraham. During that time, we have also conducted

inspections of four other non-NNSA sites that have significant quantities of nuclear material and classified information.

Our inspection process has always included assessments of the effectiveness of physical security, including alarm systems, protective forces, training and equipment, and information security including protection of documents and electronic data. We also look at protection program planning, including the site vulnerability assessments, to include the effectiveness of contractor and line management feedback and improvement programs to include the contractor self-assessments and the DOE field element survey programs.

Unlike most inspection programs, Independent Oversight has always made extensive use of performance tests in all areas that we assess. These tests range from relatively straightforward tests of the calibration of security systems, such as intrusion alarms and metal detectors, to large and complex tests of the integrated effectiveness of security systems using engagement simulation systems, more commonly known as MILES gear. We do extensive testing of cyber security systems using the same techniques that hackers use. We have demonstrated our capabilities to Congressional committee members on past occasions and have established a cyber security laboratory that allows us to continually develop and modify our techniques to keep pace with changing technologies and ever-evolving hacker methods.

Although we have been conducting large-scale force-on-force performance tests using the DOE Composite Adversary Team for over 15 years, the 9-11 events prompted us to redouble our efforts in this important area. Since 9-11, we have substantially increased the number of tests we perform. We have also increased the skills and the amount of specialized training of our Composite Adversary Team to include terrorist tactics and advanced training used by the U.S. Special Forces and foreign special operations units. We have also increased our organizational capability to perform effective tests by obtaining specialized expertise from nationally recognized experts in tactical operations and counter terrorism.

OA has also supported the development of the revised design basis threat. Other DOE organizations have responsibility for the revised design basis threat and will discuss its status. Independent Oversight is now considering how it will perform performance testing under the new design basis threat.

Current Status of Security at the Department of Energy

Based on our inspections and performance tests, I will now provide a brief overview of the status of security programs across the DOE nuclear weapons complex.

Starting out with some generally positive aspects:

- As a result of the increased security measures put in place following the attacks of September 11, 2001, DOE sites have significantly increased the level of security. They have increased the number of protective force members on duty at any given time and have further limited routine access to key areas of the sites. To accommodate the increased workload, many sites have hired and continue to hire additional personnel for their protective forces. They have also added additional barriers and hardened fighting positions.

- The classified cyber security program is maturing. After experiencing a number of problems with complex issues of protecting classified information on computer networks, DOE's performance has been steadily improving in this area for the past several years. Our inspections have found only minor issues within this program in recent inspections. However, we have seen examples of backsliding and complacency, and will continue to focus on this important area.

- Our inspections have also indicated that the protection afforded classified documents is generally consistent with national policies. Protection of classified non-nuclear parts, such as the electronic components of nuclear weapons, has greatly improved but still needs continued attention to ensure that interim measures are replaced with permanent solutions. In addition, DOE has established some more stringent requirements for certain higher priority assets (such as electronic media with particularly sensitive information) in recent years. Our inspections indicate these new requirements are an improvement but implementation is not yet uniformly effective.

Notwithstanding these positive aspects, significant work remains and our inspections have identified a number of weaknesses that need additional attention:

- The recent hiring of additional protective force personnel and the heightened security levels has created an interim set of problems. New protective force members have received mandatory training and testing (e.g., physical fitness and firearms) but the security clearance process has significantly delayed the deployment of these newly hired protective force members. Some sites have also had to defer critical performance tests because manpower is stretched to the limit.

- DOE sites have primarily responded to the need to enhance security post 9-11 by using manpower intensive measures. While appropriate as an interim solution, additional attention is needed to establish and implement more effective solutions by enhancing the integration of manpower and technology, more effective barriers, further consolidation of security assets, and extensive performance testing to ensure system effectiveness.

- Unclassified cyber security continues to be a challenge for some sites. While most sites have robust protection of their unclassified networks against both external and internal attack, some sites have not adequately addressed certain threats such as the potential for an authorized user to elevate his access privileges to gain access to potentially sensitive information on the network. We have noted recurring deficiencies with the adequacy of controls for foreign nationals on DOE computer systems; there are instances where sites did not have sufficient controls to ensure that the ability of foreign nationals to access information was thoroughly reviewed and controlled. In addition, some sites have not fully recognized and addressed the inherent risks associated with the recent proliferation of wireless technology in computer systems.

- The recent NNSA reorganization has the potential to streamline and clarify security responsibilities, and we have noted some recent improvements in this area. However, the new site offices do not yet have the staffing and expertise to be able to effectively discharge their responsibilities in the security oversight arena.

- Weaknesses in feedback and improvement processes are a long-standing concern, both within the DOE line and contractor organizations. Effective contractor self-assessments are a foundation to the ongoing effectiveness of security programs. OA inspections indicate that some aspects of contractor self-assessments are improving but there are often weaknesses in corrective action management processes, including insufficient root cause analysis. As a result, deficiencies recur. Similarly, on the DOE line management side, the reviews are not always sufficiently rigorous and do not include sufficient performance testing in some areas. The near-term staffing and expertise issues associated with the NNSA reorganization exacerbate these weaknesses.

- Protection strategies and effectiveness will need to be reevaluated when the revised design basis threat is fully implemented. DOE sites' vulnerability assessments have largely been conducted using the previous design basis threat or been deferred until a new design basis threat was prepared. Similarly, the force on force performance testing conducted by Independent Oversight has been conducted using the old threat in most cases. While it is clear that every site has increased its level of protection in response to the September 11, 2001, attacks, few of these enhanced protection schemes have been fully performance tested or subjected to quantitative vulnerability analysis to assess their effectiveness under the current concept of the threat, because the new threat policy had not been published. Therefore, the determination of whether the current programs are sufficient has largely been deferred until the new design basis threat was published.

The weaknesses in feedback and improvement and clarity of security roles and responsibilities are longstanding and have been identified on many past inspections. Progress in these areas, however, has been inconsistent and sporadic. We believe that well defined responsibilities and effective feedback programs are the lynchpin to effective security programs.

The Secretary, Deputy Secretary, and the NNSA Administrator are placing significant emphasis on reorganizing the management structure to clarify responsibilities and increase accountability. They have demonstrated personal involvement in enhancing security after 9-11 and in response to recent security lapses. For example, the Administrator for the NNSA personally requested that we perform an accelerated review at Sandia to address concerns with protective force operations. The current efforts are promising but significant continued attention and evaluation is imperative to ensure that they are sustained and the intended improvements are realized at the field level.

Closing Remarks

In closing, much has been accomplished but much more work remains to be done. This is especially true considering the more stringent design basis threat and to ensure that longstanding weaknesses in role and responsibilities and feedback programs are fully addressed. The recent strong and aggressive senior management focus on security will result in program improvements, but this effort will need to be sustained to address the challenges DOE faces.

Mr. TURNER. I would acknowledge that Mr. Dennis Kucinich from Ohio and Mr. Ron Lewis from Kentucky have joined us. And we will begin our questions with the 5-minute round, and our first questions will be asked by Mr. John Duncan of Tennessee.

Mr. DUNCAN. Well, thank you very much, Mr. Chairman. Just a little less than a month ago, the Knoxville News Sentinel had a story under the headline DOE "Again Thumbs Nose at External Safety Regulation," and the story says—this is not a new story, of course—critics have skewered DOE's self-regulating status for years, and the GAO has issued regular reports showing how external regulations would improve safety accountability and, for God's sake, save money too.

In its newest finding, they said shifting down regulation could save DOE as much as $41 million annually; and in its response, the DOE questioned cost estimates and the quality of GAO's research data.

The GAO counters with this biting conclusion that at this point, with the analysis undertaken on this issue over the years, it seems to us that philosophical opposition rather than data limitations is the main stumbling block to the Department's shift to external regulation. Indeed, same song, slightly new verse.

Is that an accurate story, Ms. Nazzaro, and would you care to comment on that? And then I will ask Mr. Podonsky if he wants to say something.

Ms. NAZZARO. I would say, yes, it is an accurate story. I mean, GAO does stand by our analysis as far as the dollar savings, which was the only thing that was disputed.

Mr. TURNER. Ms. Nazzaro, could you please come a little closer to the mic so we can all hear you.

Ms. NAZZARO. We have reported, as you said, for years on the benefits of external regulation. We continue to be supportive of that concept. And this was the first year that we had done some comparison as far as potential dollar savings, and have compared it against a pilot project actually that was done using data from another agency; and we stand by those numbers.

Mr. DUNCAN. Mr. Podonsky.

Mr. PODONSKY. Congressman, I would have to defer that answer to the Department for a response. Since we do an independent oversight of the Department, we have not actually looked at what the effects would be if there was an external regulator.

Mr. DUNCAN. Let me ask you this. The NNSA was created in March 2000, and that was 1½ years before the events of September 11. What was accomplished in that 1½ years? You said something about shifting management and so forth. Was nothing done?

And then this DBT thing, design basis threat. I have to say whoever came up with that sure came up with a bureaucratic title. But it took 2 years to issue this DBT. Why did that take so long? And what were we not doing before in regard to security that we are doing now?

Can either one of you answer some of these questions?

Ms. Nazzaro.

Ms. NAZZARO. I can start.

There was a previous design basis threat document. This isn't a new document within the Department. There was a design basis

threat document that was developed in 1999 based on a 1998 assessment. This was an updated one based on the events of September 11.

DOE decided it needed to update the prior design basis threat. What it addresses is——

Mr. DUNCAN. Even though we had a report out in 1999, it took them 2 years to come up with a report after September 11?

Ms. NAZZARO. Correct. There were disagreements on the course it was going to take, what level of risk DOE was willing to take, and what exactly the threat was.

What the new design basis threat document lays out is the level of risk and the level of threat, what is the threat as far as an adversary; and there was disagreement within the Department on what that threat would be.

Mr. DUNCAN. Well, I know from living near Oak Ridge there has always been security out there. And what I am wondering about is, you know, we have this report you said came out, this DBT report came out in 1999 and then now we have an updated one.

What I am wondering about is, what are we doing now?

Part of what I am wondering about is, what are we doing now that we weren't doing before all these reports have come out? What changes have been made?

Mr. PODONSKY. I might be able to answer that, Congressman.

Mr. DUNCAN. OK, go ahead, Mr. Podonsky.

Mr. PODONSKY. The difference between the old design basis threat [DBT], and the new one, without going into classified, the numbers have changed, "numbers" meaning what the Department is protecting against, to be more realistic with real events today. It formalizes the——

Mr. DUNCAN. When you say "the numbers have changed," are you talking about the numbers of security personnel?

Mr. PODONSKY. No, sir. We are talking about the design basis threat as a tool by which security is focusing on what it is protecting against, so how many adversaries do you need to protect against?

Mr. DUNCAN. I see.

Mr. PODONSKY. Because various threats would require different numbers. And part of this is truly for economics as well as security. You can make something so secure that you don't function any longer.

Mr. DUNCAN. Right.

Mr. PODONSKY. So there has to be a balance between your mission as well as security. And what the new DBT did, it formalized increased numbers, considering what we all saw on September 11; and it also formalized protection requirements against radiological dispersal as well as dispersal of chemical agents. So it took a look at other threats that were not previously considered under old regimens.

Mr. DUNCAN. All right.

Well, I have some more questions, but my time is up for this round, so I yield back.

Mr. TURNER. Mr. Kucinich.

Mr. KUCINICH. Thank you very much. I have some questions for Mr. Podonsky.

According to information from the Department of Energy, the National Nuclear Security Administration in 2003 estimates that they will spend $7.9 billion for their work. Is that correct?

Mr. PODONSKY. You would have to ask the NNSA. I have no knowledge of what they would be spending.

Mr. KUCINICH. OK. Do you want to tell me about the work of your department, specifically in relationship to this program?

Mr. PODONSKY. My office, Congressman, is responsible to the Secretary and the NNSA Administrator for evaluating environment, safety, and health, safeguards and security, the cyber security, the emergency management programs at the Department. We evaluate them against their requirements, but we performance test them to make sure that they are doing what they are funded to do.

For example, in the security area, we test the security forces. We look at material control accountability. We look at classified and unclassified cyber security. We look at personnel security. We look at all the aspects of the performance of the DOE and the NNSA. And then we report on that to both the inside of the Department and also to interested committees up here on the Hill.

Mr. KUCINICH. Now, there are watchdog groups, such as the Project on Government Oversight, that has alleged that force-on-force and simulated tests of nuclear facilities are dumbed down to show that security forces are adequately prepared to meet the threat. For instance, it's been alleged that security forces are given the time and, in one reported instance, even the plan of attack. Attackers are placed under artificial constraints to slow them down or otherwise limit their capabilities.

As part of your work on this project or from your experience doing other work, have you seen this happen?

Mr. PODONSKY. The answer to that is, in some cases, yes, we have seen where it has been questionable—in the past, this past year—questionable whether scenarios were shared or not shared. The reality, however, is, today I would say that we have not seen dumbed-down tests. On the contrary, we have seen very aggressive, including our own very aggressive force-on-force exercises.

The thing that is important to realize——

Mr. KUCINICH. Can you say when you have seen those? Have you personally witnessed that or have you personally——

Mr. PODONSKY. I have only heard accounts of those back in the 1997–1998 timeframe.

Mr. KUCINICH. So you don't know from your own experience?

Mr. PODONSKY. In terms of dumbed-down testing?

Mr. KUCINICH. Right.

Mr. PODONSKY. No, sir.

Mr. KUCINICH. Do you know from your own experience about the quality of testing right now?

Mr. PODONSKY. Yes, I do.

Mr. KUCINICH. Do you think the DOE has determined the design basis threat based on actual threat to the facilities; or is it influenced by budgetary constraints?

Mr. PODONSKY. We believe that the design basis threat today is a very aggressive, robust threat statement. We do have two concerns that I will be happy to talk about under closed classified session. But overall we think, given today's threat in the world, the

DOE has a very high mountain that it has created, and we think it is very appropriate.

Mr. KUCINICH. Thank you.

Mr. Chairman, I have here a copy of an attachment that includes a Department of Energy budget. I think it would be interesting for the people of this country to know that nearly $8 billion is estimated to be spent on the National Nuclear Security Administration, and that environmental management, which doesn't include a certain amount of cleanup, is scheduled to be about $7 billion—nuclear waste disposal, about $591 billion—or million.

When you look at this overall budget, Mr. Chairman, there is a question that just needs to be raised in the context of this hearing, and that is the policy of our government with respect to building nuclear weapons in the first place. And while this is about the threat that derives from having produced such weapons, it appears that the weapons that we are producing, far from being a threat to other nations, end up being a threat to ourselves. Just a little thought for today.

Thank you.

Mr. TURNER. Mr. Lewis.

Mr. LEWIS. Thank you Mr. Chairman. Ms. Nazzaro and Mr. Podonsky, how adequately staffed are DOE and NNSA for insurance safeguards and security at the nuclear weapons complex sites?

Ms. NAZZARO. In regards to staffing, the issue we looked at was staffing as it relates to oversight, and that's where we found that there was a deficiency as far as capabilities to conduct oversight of the contractors. DOE's response has been that it will use this virtual organization whereby they would use individuals from other locations to conduct oversight.

However, we do have concerns that the staffing certainly is inadequate, and they do have a number of vacancies that need to be filled. But we looked at it only in that aspect.

Mr. LEWIS. Thank you.

Mr. Podonsky, what are DOE and NNSA doing about the staffing problem?

Mr. PODONSKY. To the NNSA and DOE's credit, they have increased the personnel in terms of security guard force, which was very important.

Relative to staffing at the sites for, as Ms. Nazzaro was talking about the self-assessment oversight, the programmatic oversight, they are taking a very rigorous approach to try and find more staff.

We fully agree with the GAO from an independent oversight perspective, that there is a need, a very serious need, at all the site offices to beef up the staffing with qualified, capable folks to oversee the contractors, as well as the contractors to oversee themselves.

Mr. LEWIS. And what's the problem in getting the staffing up to par, finding qualified people? Or what's the problem?

Mr. PODONSKY. Well, you would have to ask the NNSA or DOE directly. But I would give you our opinion from independent oversight which is, there are a lot of competing concerns for security in the country today and it is very difficult. I know in my own organization to maintain and keep very highly qualified national-level experts in the security business and to attract them into govern-

ment service is quite difficult because the salaries are not necessarily as attractive as they are in the private sector.

Mr. LEWIS. OK. Thank you.

I yield back my time. Thanks.

Mr. TURNER. Mr. Chairman.

Mr. SHAYS. I thank you all for being here. Let me ask you, Ms. Nazzaro and Mr. Podonsky, how do you define adequate security? And let me just say, we are talking about security in our labs, our production facilities, our test sites, and the closed-down environmental sites.

And how would you define adequate security?

Mr. PODONSKY. It's very——

Mr. SHAYS. And maybe in your answer you can tell me the different kinds of security we're talking about.

Mr. PODONSKY. Well, at the Department of Energy, security has been a focus through various ebbs and flow in time. Back in the 1970's, it was heavily focused on security and there were changes that were made.

In the 1980's, safety was focused on. In the 1990's, more safety. And then, of course, post-September 11, security was focused on again.

And I would just tell you that adequate security really depends on what is being protected. And from our standpoint, the Department, now more than ever, is focusing on providing appropriate security while still trying to maintain its mission.

If you talk to security professionals, they would give you an answer that may be unacceptable in terms of what type of budgets would have to be spent to provide the adequate security that they may need.

It's similar to what TSA is going through at the airports. How many security screeners do you need? What's appropriate for what you're trying to do? And the airlines will tell you that they're trying to make sure the passengers make it to the airplanes on time.

In the Department of Energy, we have different sites, different categories of protection, and the security and the design basis threat that we've talked about here is tailored to meet those needs. Again, I would say that the adequacy is difficult to pinpoint because it changes, dependent on what the target is and what you're trying to protect and what your mission is.

Ms. NAZZARO. Without getting into any classified information, what we would look at are two levels: One, there are a number of assessments that are performed to look at the adequacy of security, both surveys and surveillance that DOE uses; and we would expect that those would be clean assessments, you know, and that any action plans that were identified as a result would be addressed.

Second, they do identify a level of risk. And DOE does have various levels of risk, and we would expect those to be at the lowest level, as set out in DOE's policy.

Mr. SHAYS. Tell me, if we don't have adequate security, what are the potentials that could be used by governments, their spy networks or by terrorists, to—I want to know why this matters.

It may seem obvious, the question, but I want someone to articulate it. Why does all this matter?

Ms. NAZZARO. Well, there are certainly a number of threats—I mean, one being theft of nuclear weapons and/or materials; also, sabotage at the sites themselves. Certainly, within a terrorist environment, you've got people who are willing to die to go and actually detonate these at the sites.

Mr. SHAYS. But just going from your response, we're talking about the potential that someone could actually get a nuclear weapon; is that correct?

Ms. NAZZARO. Correct.

Mr. SHAYS. We're talking about the fact that they could get weapons grade material?

Ms. NAZZARO. Correct.

Mr. SHAYS. We're talking about the fact that they could come onsite and sabotage the sites?

Ms. NAZZARO. Correct.

Mr. SHAYS. And we're also talking about the fact that they could potentially cause a radioactive catastrophe or a nuclear explosion?

Ms. NAZZARO. At the sites. Correct.

Mr. SHAYS. Yes. So that's why we care about this?

Ms. NAZZARO. Yes, sir.

Mr. SHAYS. We're also concerned with countries, other countries getting the technology that, in many cases, they may not have at all, or that they may be 10 or 20 years behind us. Is that also a factor?

Ms. NAZZARO. Yes.

Mr. SHAYS. OK.

When you did this report, I was—some of it seems—I don't want to say "technical" in that sense; I want to say that I was wondering if we were swallowing camels and straining out gnats. When DOE looks at this, do they—is their response to you that—you know what? I will come back. After you've had your round, I'll come back for my round. I want to followup on this question, and my time is up.

Ms. NAZZARO. OK.

Mr. TURNER. Thank you, Mr. Chairman. I think it is very important that you were asking the question, why does this matter, because if you look at the report that we have in front of us, it certainly does not reflect the—I think, what people in our country would consider the severity of the issue or the attention level that this deserves not just as a threat to Americans, but the possibility of the threat to others of technology, of even other countries being threatened by materials that we have through individuals that might seek them.

In looking at Ms. Nazzaro's statement, you have issues, such as stating that defining clear roles and responsibilities has not been effectively done; assessing the site security activities needs to be addressed; overseeing contractors; corrective actions; allocating staff—all issues or problems.

When you look at issues of our nuclear materials, you would expect that we would be able to use words such as "proactive" and "advanced." What we're clearly seeing in the materials in front of us are words such as "slow" and "incomplete."

And I'm just wondering, if you look through there—and clearly it's unacceptable, so you have to ask yourself, is it an issue of

structure? Is it an issue of people just don't understand the severity of the issue in front of them? Is it a performance issues?

So I would like Ms. Nazzaro and Mr. Podonsky to tell us.

I mean, I'm certain that it is not acceptable, that this—reading this, you agree that this is not where we would want to be, and this is a concern for all of us.

Where is the problem, other than just saying the problem needs to be fixed? Is it structure? Is it understanding the mission? Or is it just a straight-out performance issues and somebody needs to be held accountable there?

Ms. NAZZARO. The report you have in front of you addressed management and oversight issues, as far as DOE and NNSA overseeing the activities of the contractors.

Some of the things that you're getting into would be more contractor performance issues, which we have not yet addressed; and that will be the subject of followon work, actually, that Congressman Shays has asked us to do.

As far as the issues, though, at hand, you're still talking about safeguarding and protecting the nuclear complex; and given the kinds of materials that they are in charge of protecting, you know, this is something that is critical to the country. I mean, if you don't have adequate management and oversight of the contractors, you're going to see problems with the contractors as well. So I don't think it minimizes it by saying, these are the kinds of problems we're seeing. It certainly is an overarching issue of whether you're even overseeing or managing what the contractors are doing.

Mr. TURNER. I take it from your answer, in looking at NNSA's management oversight, it's an agency performance issue at this point, you believe; or you're indicating that you think additional information has to be given for you to define why is this continuing to be a problem.

Ms. NAZZARO. No. As far as DOE, certainly we have seen ongoing problems for some time, since the creation of NNSA. As we said, this has been an agency in flux, and we have seen problems as far as defining roles and responsibilities where it's not clear who is supposed to do what; and basically what we have heard from the site offices is that they're all doing the wrong thing.

Mr. TURNER. Mr. Podonsky.

Mr. PODONSKY. I would start out by saying, many items in the GAO report the independent oversight does, in fact, agree with. However, I think it's important to note that Secretary Abraham and Ambassador Brooks are aggressively taking steps that have never been taken before in the Department, as long as I've been there—which is going on, unfortunately, about 19 years of overseeing this behemoth organization. And the step that they are taking is, they are—finally, somebody is being held accountable. We're seeing this at our national laboratories. We're seeing this at the sites.

If you ask, Congressman, what's the root cause, I would tell you that—my organization, after observing and writing reports on these very issues for many years, would tell you that roles and responsibilities have not always been clear; and the accountability, which is a critical part, has not always been taken where people were

held accountable for those jobs that they hold. So it is a performance aspect, as well as management.

But I would again iterate, the Secretary and the Ambassador are taking steps which we're seeing firsthand. We have teams out at some of the NNSA sites right now at the request of the Ambassador. Now, how that trickles down to the other managers in the security profession, that's where the rubber meets the road; and we think that's where further accountability has to be made.

Mr. TURNER. Thank you.

Going to a second round of questions then, Mr. Duncan.

Mr. DUNCAN. Let me just ask this. You know, any time any government agency—I don't care what department or agency it is, any time they mess up, they always come in and say it's because of lack of funding or not enough money. And yet, we've had 10 or 15 years of very low inflation. In fact, the Federal Reserve is worried about deflation now. We've probably had 25 or 30 percent inflation over these last 10 years, and yet whenever you look at these agencies and ask what they're spending, compared to 10 years ago, they're at 60 and 100 percent over what they were 10 years ago.

I remember when the INS was criticized because they let all the hijackers in. They said they didn't have enough money, and we checked and they'd gotten a 250 percent increase in funding over the previous 8 years, which—I mean, this just boggles my mind that we hear this over and over again.

Now I hear that the NNSA, which was just started in 2000, March 2000, has a $7.9 billion budget. And I—you know, that's—I'm all for saving all the money we can, but you know, and now we're acting like we're not doing enough in security.

And Mr. Podonsky just said that we're doing far more than at any time in his 19 years at the Department. And I'm just wondering—you know, I don't want to scare people and think that we're not doing enough at these nuclear weapons facilities, and I'm curious about several things.

I've read several times, I've read different numbers, when—about the Iraqi war, and that there were 23 or 25 countries that have weapons of mass destruction. Does anybody on this panel know how many countries have nuclear weapons? How many countries are there that have nuclear weapons facilities? Do any of you know that?

Ms. NAZZARO. I wouldn't have a total number, no, sir.

Mr. PODONSKY. No, sir.

Mr. DUNCAN. Well, what I'm getting at, is there any country in the world that's doing more in regard to nuclear weapons facilities security than we are? Or any country that's doing even close to as much as we are? Surely somebody knows that question.

Mr. PODONSKY. I would believe that this country is doing, probably, the most of any.

Mr. DUNCAN. Probably by far?

Mr. PODONSKY. By far, yes, sir.

Mr. DUNCAN. And I'm not really clear on this. The NNSA budget, which is $7.9 billion and is all pertaining, supposedly, to security—because, I mean, that's what it's set up for. But how much is the DOE spending on security in addition to this $7.9 billion? Do you have any idea on that?

Mr. PODONSKY. I don't have that figure, no, sir.

Mr. DUNCAN. But I assume that's a very large figure also.

Mr. NOEL. Actually, out of the NNSA budget, $8 billion, about $580 million is devoted to security. The balance is for operating the complex, protecting nuclear materials in other countries like the former Soviet Union, and producing naval reactors that operate in our ships.

Mr. DUNCAN. So we're providing the security for other countries, as well as ours?

Mr. NOEL. No, not in this way.

Mr. DUNCAN. Or just the Soviet Union?

Mr. NOEL. We are helping the former Soviet Union secure plutonium and highly enriched uranium so that terrorist groups cannot get their hands on it.

But providing the actual physical security or overall security at the NNSA facilities is about a $580-million-a-year operation.

Mr. DUNCAN. One of the things I'm concerned about is that I remember just a few weeks after the events of September 11, 2001, former Congressman Callahan, who was the senior member of the Appropriations Committee, said in a meeting that I was in that he—he said, and very sad about it, I guess—he said that he estimated roughly that we would spend $1.5 trillion over the next 5 years on security matters, all throughout the government, that we wouldn't have spent otherwise.

And the Wall Street Journal had an editorial after we passed the farm bill that we called the Farm Security Act, and they said that every department and agency was requesting—was using the threat of the incidents of September 11 to greatly increase their funding; and they said, from now on any bill that has the word "security" in it should get four times the scrutiny.

And, you know, when you think about it, if we go—Mr. Podonsky hit on this a few minutes ago when he said, we have to have some sort of balance here between some reasonable security, but not interfering with the overall mission of the agency. And I think this was—he may not have meant that to be one of his key points; but I think it was, because in some ways, we're going ridiculously overboard on security and wasting all kinds of money that could be being spent on many other really good things.

And I just wonder, are we achieving the balance that we need here?

Ms. NAZZARO. Well, I don't think DOE has gone through that whole process yet. The design basis threat was the first step to identify what is the threat.

Mr. DUNCAN. Well, what's left that we have to do? You said that there was a Design Basis Report issued in 1999. Then they spent 2 years on a new design basis threat. I mean, are we just going to have report after report after report?

Ms. NAZZARO. No. The next step now would be to look at what it would take. They've raised the bar as to what this threat is; now they need to look at what it will take, what will be the cost versus the benefit that they will get from improving their systems; and there will be a certain level of risk that they will just accept that cannot be addressed. It may be too cost prohibitive. But we have identified a number of things that the agency should be looking at

including, you know, closing public access, either acquiring more land around the facilities, closing roads, public roads that go into the facilities.

Another thing they could do is close facilities that are no longer needed. Certainly there will be the development of new facilities in the use of new technologies, in some cases which may be more costly than currently in place. But there are some other things that can be done that, you know, are more cost efficient.

Mr. DUNCAN. Mr. Podonsky did touch on it when he said that, you know, you can have so much security that you just really shut down a facility or you stop what's going on. And that—I mean, I know it's a very difficult question.

Mr. Podonsky, do you have any comments?

Mr. PODONSKY. Well, I think you're making the point of what I was saying in my opening remarks and that is, there has to be a balance and the Department is going through this assessment. Now that they have a design basis threat, they know what they are protecting against. They have the numbers. Now they have the data with strategies and use of technology, and we would agree that throwing or putting more money into the system is not necessarily the only solution to meet the security threats that you're trying to protect against.

Mr. DUNCAN. We do have to take security very seriously, and I want to do that. On the other hand, I read 2 or 3 months ago an article, or column, that said we have forgotten the fact that we're wanting to protect so much against terrorism that people are still 99.99 percent more likely to be killed by something else like cancer, heart disease, car wrecks, things like that; and we're spending trillions or hundreds of billions on security against terrorism to the neglect of things like more safety on the roads and more research on cancer and heart disease.

And, I mean, we've got to get a hold of ourselves at some point.

Ms. NAZZARO. You made a good point, and I think that supports our finding where we said that the agency has not addressed the corrective action plans appropriately. They have not done cost-benefit analysis. They have not, you know, assessed the risk level. They have just gone forward without, you know, really looking at what was the root cause of the problem before they took corrective actions.

Mr. DUNCAN. Well, we just not only—"balance" is the key word, but also common sense is something else that we seem to be lacking on some of these things.

Thank you, Mr. Chairman.

Mr. TURNER. Mr. Lewis, we are going to go to a 10-minute round of questions so if you'd like to take——

Mr. LEWIS. I have no questions.

Mr. TURNER. Mr. Chairman.

Mr. SHAYS. Thank you.

I know it's been asked and I know it's been responded to, but I want the four of you, to tell me why a design basis threat is an important document.

Mr. NOEL. Well, basically the design basis threat sets the minimum standard to which the facilities have to be protected; and it lays out——

Mr. SHAYS. We're talking about all the facilities, the labs, the environmental cleanup sites, the production sites, all of them, the test site?

Mr. NOEL. Right. It applies to all of the department's facilities. Now, it will apply in different ways. Clearly, a facility that has a nuclear weapon or nuclear materials will be protected to a much higher standard than a facility that is being cleaned up and just has waste materials there. But it is the standard by which the facility is going to be evaluated. It is the standard to which the contractor has to operate. So it forms the minimum to which these facilities need to be protected.

Mr. SHAYS. Plutonium, a weapons grade—enough weapons grade material of plutonium is the size of a large orange, and if it's sealed, you can touch it, but it's not all that large. Highly enriched uranium, I could touch. It is the size of a large grapefruit, weighs about 30 pounds, but neither give off any noticeable smell, you know, just dirty radioactive material, and so we're not talking about a truckload to cause the damage. We're talking about what someone could basically carry out. We are talking about facilities that have developed weapons that enable us to use small amounts of this material and cause horrific explosions.

We have had testimony in this committee that terrorists could basically detonate a nuclear weapon, if they didn't mind going up with it, and not all that sophisticated equipment, a weapon. So if you were to—and so I'm kind of responding to Mr. Duncan. I happen to agree that we could protect our citizens on a whole host of different levels for a whole host of different things and go bankrupt and have the economy not move forward and have poverty, not have breakthroughs in medicine and so on, but when we're talking about these facilities, we're talking about a potentially catastrophic outcome if terrorists get weapons grade material, if terrorists get a weapon or if terrorists actually get into these sites and are able to cause some real danger.

Did either of you come to any conclusion about which sites were more vulnerable—the labs, the production facilities, the test site, the old environmental cleanup sites? Have any of you tried to assess where we are most vulnerable? And if we have—and if that is not for public consumption, we can deal with it later.

Ms. NAZZARO. I would say we would want to discuss that this afternoon, sir.

Mr. SHAYS. But this part you can say publicly. Do you all have a sense of what you consider most vulnerable within those four categories?

Ms. NAZZARO. I would say we have some examples that we could provide.

Mr. PODONSKY. Congressman, for the Secretary's oversight, we do know what we believe are the more vulnerable sites and which are the more protected sites, and we would be happy to discuss that with you in closed session, but we do have that information.

Mr. SHAYS. Now, do each of the sites—can you group the production sites together and say that you have the same basic problems in the four—I think we have four sites or the three labs. If you have a problem with one lab, is it somewhat consistent with an-

other, or are we going to have testimony behind closed doors that particular sites may be more vulnerable?

Mr. PODONSKY. From our perspective, each site has its own unique characteristics.

Mr. SHAYS. But do they have similarities if they are labs versus production facilities?

Mr. PODONSKY. There are similarities both within the labs and also crossing over into the production sites. So we may have a problem that we have identified at a lab and it may also be a shared problem at a production site, as you refer.

Mr. NOEL. Mr. Chairman, it really has to do with the materials and which facilities have which materials and how those materials might be used. So it's not a function of necessarily what the place does but the materials they use.

Mr. GILL. And also, too, how the facility is configured.

Mr. NOEL. I think it's important to recognize that this concern extends beyond NNSA but to the department as a whole, including some of the facilities in the Office of Environmental Management.

Mr. SHAYS. When I go through, I sometimes am told there are 12 sites, there are 11 sites, there are 10 sites, depending on what document I look at, and so it does get to be a little frustrating. Why am I given different numbers?

Mr. NOEL. Maybe I could help you out with that. In the NNSA's nuclear weapons complex, there are basically three design labs and four production plants and the Nevada test site.

Mr. SHAYS. OK. So those are the big eight.

Mr. NOEL. With their world. In the Office of Environmental Management, there's roughly about eight large cleanup sites. For the purpose of our——

Mr. SHAYS. Let me ask you, are some of those cleanup sites on any of the eight that you mentioned, or are they eight additional sites?

Mr. NOEL. Unfortunately, they are. The Savannah River site is both a cleanup site and a weapons production site.

Mr. SHAYS. So it's a double counting on my——

Mr. NOEL. Yes. For the purpose of our analysis, we went to all DOE sites that have what are called category I special nuclear materials, and that is basically plutonium and highly enriched uranium that are the materials of interest that you were discussing.

Mr. SHAYS. And in those two instances, none of the cleanup sites would have those, correct?

Mr. NOEL. No, unfortunately, they do. Hanford, Rocky Flats, Idaho and Savannah River all possess Category I special materials.

Mr. GILL. And also, too, Mr. Chairman, not all the NNSA sites possess category I materials. The ones that do have category I materials: Los Alamos, Sandia, Livermore, Y–12 and Pantex.

Mr. SHAYS. The other thing that I was blown away by was that some of these facilities, they don't have 20 buildings, but if—I read this when I was in the plane last night at 2:30 at night, but I think I read, 200 buildings, 300 buildings. I mean, why so many buildings at these sites?

Mr. NOEL. Well, these facilities have been built up over a long period of time; and, you know, if you go to some of them—the first time I went, somebody said, well, think of like a 50-year-old fac-

tory, and that's what you're going to see, and that's about what a lot of these places look like. But the facilities that actually have—within the site, the facilities actually contain the materials of interest, that is a much smaller number, and the materials tend to be consolidated in certain buildings and then——

Mr. SHAYS. So I shouldn't be exercised by the number of buildings that——

Mr. NOEL. No, I don't think so.

Mr. SHAYS. But Los Alamos, 43 square miles. The Hanford Site, 560 square miles. The Savannah River Site, if I'm reading this correctly, 300 square miles.

Mr. NOEL. Yes. The overall site is——

Mr. SHAYS. Idaho, 888 square miles.

Mr. NOEL. Yes. And the issue there—and Mr. Podonsky can talk about this a little bit—is, you know, that provides an enlarged area in which an adversary might be able to come closer to the site and to the actual materials than you would—of interest to him without potentially being detected till he was very nearby.

Mr. SHAYS. Well, let me just ask, do the number of buildings and the size of these facilities create additional problems? Obviously, the more buildings you have, that creates problems, but—in terms of security and so on, but is the size something that is a benefit because then we can have a no-man's-land area that—I mean——

Mr. PODONSKY. Congressman, it is a double-edged sword. In some cases, from a security posture, the size is helpful. The other side is you want to start consolidating the target, the nuclear materials, and that is what the department and the NNSA is starting to do.

We saw an example of this, actually—the department doing this prior to September 11 at the Hanford Site where they consolidated their—what we call the target to just a few buildings, and they continue to do that.

The same thing is going—is happening at the Y–12. People are looking to consolidate and to reduce the exposure, if you will, to hostile elements.

Mr. SHAYS. We have some questions that the committee has written up that we need to ask, too, but maybe—pardon me? OK. We can submit them.

Thank you, Mr. Chairman.

Mr. TURNER. I want to thank the panel. I don't have any other questions. I appreciate your participation today.

We'll move on to our second panel.

Our second panel will consist of Linton Brooks, the Administrator for the National Nuclear Security Administration, Department of Energy; and Joseph Mahaley, Director, Office of Security, Department of Energy.

We're waiting for Mr. Mahaley to join us.

Mr. SHAYS. We told him 11 o'clock, so he is not technically late.

Mr. TURNER. I'd like to also at this time acknowledge that Mr. Tierney has joined us, and Mr. Ruppersberger had also joined us for part of the hearing.

He is here, Mr. Mahaley.

If both of you would please stand, we'll administer the oath. Please raise your right hands.

[Witnesses sworn.]

Mr. TURNER. Please note for the record that the witnesses responded in the affirmative.

Mr. Brooks, Ambassador.

STATEMENTS OF LINTON F. BROOKS, ADMINISTRATOR, NATIONAL NUCLEAR SECURITY ADMINISTRATION, DEPARTMENT OF ENERGY; AND JOSEPH S. MAHALEY, DIRECTOR, OFFICE OF SECURITY, DEPARTMENT OF ENERGY

Mr. BROOKS. Thank you, sir. I appreciate the opportunity to appear today to discuss the NNSA's safeguards and security program.

Before I move to my remarks, I want to say that, although I'm the one who is here, Secretary Abraham is deeply committed and deeply involved in ensuring that we have an effective safeguards and security program. I meet with him and the Deputy Secretary on these issues frequently.

What I'd like to do, if I may, sir, is submit my written statement for the record and proceed with an oral statement.

Mr. TURNER. Please.

Mr. BROOKS. Mr. Shays was speaking of some of the confusing aspects of the National Nuclear Security Administration, so let me clarify what my administration includes and what I'm responsible for.

We are a separately organized component within the Department of Energy created by the Congress in response to security concerns in the nuclear weapons complex. I'm responsible for the Sandia, Los Alamos and Livermore National Laboratories; for the production plants at Y–12 in Tennessee; the Pantex plant in Texas; the Kansas City plant, which does only nonnuclear work in Kansas City; for the Nevada test site; and I'm responsible for some portions of the Savannah River site where we process tritium. I'm also responsible for the Office of Secure Transportation, which moves all special nuclear material and all weapons.

I am obviously part of the Department of Energy and bound by DOE orders, but the law provides that no official of the Department of Energy other than the Secretary and the Deputy can give me direction. I operate my own safeguards and security program following the policy that is developed by the department, by Mr. Mahaley.

I have eight site offices at the eight facilities I just mentioned staffed by Federal employees, and they are supported by a service center which is being consolidated in Albuquerque. Our fiscal 2004 budget request is $8.8 billion, with over 2,400 Federal employees and about 55,000 contractor employees; and from that you correctly deduce that most of what we're trying to do will in practice be done by nongovernment employees. We are, except for the Office of Secure Transportation, an oversight organization primarily.

Although we are semiautonomous, we make very effective use of Mr. Podonsky and the Office of Independent Oversight and Performance Assurance. One of the good early decisions was not to try and have my own office like that but to use Mr. Podonsky. That gives me both the benefits of complete independence, since he doesn't work for me, and substantial experience.

I share Mr. Podonsky's general perspective that we have made very good progress, but there's a good deal more to bring all elements of the complex to the level of effectiveness we desire.

In that regard, in recent months we've had a series of specific problems with security. In each instance, I believe we've taken immediate and aggressive action. Either I or one of my top managers has been engaged directly with our site managers and with the appropriate laboratory director. In some cases, I've dispatched senior teams to laboratories.

Nonetheless, I am concerned by the pattern. Although one can look at individual events and reach varying judgments about their severity, I'm concerned by the pattern, and therefore we will shortly announce—"shortly" means sometime in the next 2 days—a series of steps to improve security.

First, we will augment Federal and contractor security experts to make sure that we are effectively responding to some of these problems.

Second, we will direct our site managers to increase surveillance and to provide periodic reports personally to me to make sure that I understand what they're finding.

Third, we've been the subject of a large number of external reviews. We think we've implemented most of the recommendations. We'll go back in a systematic way, look at every review, look at every recommendation, say did we implement it and, if we didn't ask, do we want to rethink that?

Fourth and fifth, we will form two groups headed by senior outside individuals, one to look directly at physical security and see whether there are patterns to these problems and one to look at people.

You heard in the last panel concern about staffing. I share that concern, and I particularly share the concern over the long term. I have some extremely confident people in safeguards and security, one of whom's common characteristic is they could retire very soon, and I need to look at what I do over the long term to make sure that 10 years from now my successor is not sitting here having to talk about the same problems.

Retired Admiral Richard Mies will lead the panel that looks at physical security, and retired Admiral Hank Chiles will lead the panel that looks at personnel. Both of these retired four-star officers are respected professionals in the nuclear business. Both of them have commanded the U.S. Strategic Command. In addition, Admiral Chiles led a congressionally mandated commission to look at weapons design personnel, and I'm looking for him to do the same thing in security personnel. The Secretary and I are very pleased that they have agreed to take on this challenge, and we think they will help us make sure we have the optimum safety and security system for the 21st century.

I'd now like to address the various points that you specifically asked that we cover in our testimony.

First, you asked what did we do after September 11. Well, the most obvious things we did immediately were to execute our predetermined emergency operations plan, stop weapons shipments, and deploy emergency response assets. Then my predecessor di-

rected a short 24-hour security review and then a longer 72-hour review of potential vulnerabilities.

The results are classified, but we have used them to reduce our vulnerability. For example, in the last panel you heard comments about closing roads. We've closed roads, and we're in the process of closing other roads.

And then over a somewhat longer term, we assembled a team of subject matter experts to look at a whole variety of things, and once again we are implementing on a systematic basis those recommendations.

Since September 11th, we've continued to strengthen our capabilities. As was mentioned in the last panel, we've increased protective forces. In the year 2000, we had 1,780 protective officers. Now we have 2,160. We've added barriers, we've closed roads, we've increased security patrols, we've increased access patrols, and we've increased employee awareness. And in addition we are, as you heard on the last panel, continuing to look at how to consolidate materials.

Let me turn now to the report released this morning by the General Accounting Office on NNSA's Safeguards and Security Program.

First, I believe that the GAO did concentrate on the right things. I believe most things in life are a question of management, and this is clearly a question of management. If we do not get the management of safeguards and security right, we will never fix the problem. So I believe the GAO was looking at the right issues. They made four broad recommendations, three of which I agreed with.

First, the GAO suggested formalizing roles and responsibilities. Those on the panel with past experience with the Department of Energy will know that this has been a historic problem within the Department, and so I agree we have to make absolutely clear to headquarters for the field program, contractor personnel what the responsibilities of each are. To that end, in December 2002, I implemented a major reorganization. That reorganization eliminates an entire layer of management, puts the site office manager as the clear, responsible and accountable Federal official at each site and makes that officer report directly to me.

In addition, as GAO recommended, last month we issued a specific functions responsibilities and authority manual for safeguards and security to clarify at a working level detail who does what.

I think these steps address the first of GAO's recommendations, but I think that it is incumbent upon me and my subordinates to be vigorous to ensure that the lack of clarity in roles and responsibilities, that being one reason they created NNSA, doesn't recur.

In particular, you heard a comment from GAO about site offices, saying that they all did things differently. The comment is based on 18-month-old data. I would be delighted with no advance notice to have anybody call my eight site office managers now and see if they believe it is still the case. I do not believe it is still the case.

Second, the GAO suggested that we pay greater attention to contractor corrective action plans. This is one of those things that sounds mundane, but it's actually quite important. Finding problems is appallingly easy. Fixing problems requires sustained effort.

While we may disagree slightly with the extent of the problem, to the extent that there are problems with contractor corrective action plans, we will redouble our efforts, and one of the reasons for trying to bring in additional personnel is to make sure that we are doing so.

Finally, GAO expressed concern about Federal staffing for safeguards and security, and I agree that effective Federal oversight demands not just numbers but quality. We have reviewed with each of the site managers their allocation for safeguards and security. All believe that their current authorized staffing level is sufficient.

One, however, of my site managers, although the authorized level is sufficient, has been facing severe recruiting problems, and that is the Los Alamos site. The Los Alamos site has less than half of the safeguards and security professionals. I'm looking at what I can do about it. It is an isolated but high-cost area, which means that recruiting historically has been difficult there.

We're going to continue to monitor this, obviously, but, in addition, I believe that the initiatives that I mentioned earlier will help us understand how to make sure that we have the adequate work force.

One area in which I disagree with the GAO sounds technical, but it actually has a fairly strong policy component. The General Accounting Office recommended that we use a technique called "surveys" rather than a technique called "surveillance" in providing our oversight. Surveys involve a 2-week, once-a-year, onsite visit, a very complex, very formal—there's an entry conference. There's data collection. There's outbriefings. There's a report. But it only happens once a year. Under surveillance, we spread out the work and do periodic surveillance throughout the year. We believe that the surveillance approach is equally effective.

However, the GAO is correct that the current department order does not support the approach that we are using. The current department order does not make surveillance an acceptable alternative.

Mr. Mahaley and I have discussed that issue. We are both in agreement that the department order should be changed to legitimize the practice. The practice is right, but it is very important in safeguards and security that you're following the rules, since, after all, that is what you're trying to do, is make sure the rules are being followed.

Mr. Mahaley will speak this afternoon and briefly today on the design basis threat. Let me just say one or two words about it.

As you heard in the last panel, the design basis threat characterizes potential adversary threats for facilities. A question was asked about why you need it, and the answer is simple. Otherwise, you will have eight different people deciding how much of a threat to guard against; and some of them will be wasting resources by overguarding; and some of them will be incurring risk by underguarding. So you need a standard.

We worked closely with the Office of Security in developing the document that was produced last month. I believe it accurately portrays what the intelligence community is telling us about the threat, the nuclear weapons material and classified information.

I have heard suggestions that the design basis threat was tailored to what we believe we can afford. As far as I know, that's completely untrue. Certainly at no time in NNSA deliberations was there any suggestion of, well, we can't accept this because we can't afford it.

I don't know what the new design basis threat is going to cost. At some of my sites, I think I'm probably already there. At some of my sites, I'm going to have to spend some more money. The threat document provides for implementation over a 2-year period, as is appropriate, and I don't fully know what the cost is, but, whatever it is, we're going to pay for it, because it's too important not to.

In conclusion, Mr. Chairman, although I believe that the security posture of our complex is effective, I don't believe that we're an attractive target to those who would try to steal weapons or steal materials or steal classified material. There continue to be improvements that are required. Secretary Abraham and I are committed to making those improvements.

Since I assumed this job last July, I've been focusing personally and have focused the attention of my headquarters and field officials on insuring that our protection against theft and diversion of nuclear weapons, classified and sensitive material is robust and effective. I don't think there's any room for failure in this program, simply because the consequences of a terrorist act against one of our nuclear weapons sites are almost incomprehensible. So I intend to continue to work this problem vigorously.

Thank you for the opportunity to testify today, and I look forward to your questions.

Mr. TURNER. Thank you, Ambassador.

[The prepared statement of Mr. Brooks follows:]

Testimony of Linton F. Brooks, Under Secretary for Nuclear Security and Administrator, National Nuclear Security Administration
Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations
Hearing on Emerging Threats: Assessing Nuclear Weapons Complex Facility Security
Tuesday, June 24, 2003

INTRODUCTION

Thank you Mr. Chairman. I appreciate the opportunity to appear before your Subcommittee to discuss physical security at our nuclear weapons facilities. Secretary Abraham and I are committed to assuring that the security at our nuclear weapons facilities remains strong and effective to protect the American people and our national security assets.

A central focus of the NNSA, since its establishment in 2000, has been on security and the improvement of our overall program management. Numerous internal and independent evaluations of the effectiveness of our physical protection systems across the NNSA, including on-site inspection, rigorous force-on-force exercises, in-depth analyses and evaluation have verified that the overall security posture is strong and that we have made changes to address the security challenges in the aftermath of the terrorist attacks of September 11, 2001. While we have made progress, we know that we can make additional improvements.

We are actively engaged in addressing issues identified through formal internal and independent reviews. Overall, I strongly believe that the physical security at each of our sites is, and will continue to meet our security challenges.

The protective forces throughout the nuclear weapons complex are exemplary. These professional men and women protect some of the nation's most critical assets. Since September 11th the demands on these forces have increased, and they have responded in kind. During the nation's elevated security conditions, our protective forces have logged numerous hours of overtime a week, while maintaining utmost diligence. I therefore, continue to be very proud of the men and women who protect the nuclear weapons complex.

I would like to outline the basis for the physical security programs at our sites, the improvements we have made and continue to make since the attacks of September 11, and to address the issues identified in your hearing invitation, including those in the draft GAO report (GAO-03-471).

SECURITY ACCOMPLISHMENTS SINCE 9/11

Immediately following September 11, then Administrator John Gordon visited each of our most critical facilities to review security measures, both those in place and those planned for implementation. Within days NNSA completed a Vulnerability Assessment of the nuclear weapons complex and an NNSA Counter-terrorism Task Force was established to review current policies and operations. The NNSA also initiated a "Red Team" review of nuclear weapons facilities, known as the Iterative Site Analysis (ISA) Process. It involves in-depth planning and information gathering meant to simulate the activities of real-world adversaries. These were followed by weeks of uninterrupted analysis and table top security exercises using departmental and special operations personnel to test to failure the sites' security by going above the Design Basis Threat.

Specific actions taken at the sites include:

- Hiring additional guard force personnel to man increased numbers of posts
    - on-hand protective forces, from 1,780 in 2000 to our current strength of approximately 2,165
- Enhanced physical protection measures such as vehicle barriers and searches; use of explosive detection devices and dogs
- Increased stand-off distances from buildings and road closures
- Additional security awareness and threat awareness training for employees
- Reconfiguration of storage vaults
- Increased access controls
- Consolidation of nuclear materials, assessments, and plans for additional improvements such as road-closures/reconfigurations
- Revisions to procedures for elevated security conditions (SECON)

In January of this year, the NNSA issued the Security Condition (SECON) Policy Implementation Letter to clarify requirements for NNSA facilities, when changing security protection levels consistent with the Department of Homeland Security threat levels.

Protective Forces

Protective measures at NNSA sites result from an interpretation of the threat by the potential adversary, which is described in the Design Basis Threat (DBT) document. I understand Mr. Mahaley will provide information about the DBT and the process by which the Department arrived at the new DBT. It is important to understand, however, that the DBT is the principal factor which influences how we provide security to our sites

and how much security we provide at each site related to its relative "attractiveness" with respect to potential targeting by terrorists. Following the determination of the DBT a process that my office was fully engaged in as it was developed by Mr. Mahaley, we use a number of tools to understand what its implications may be. Those tools include vulnerability assessments of various types, which can include "force-on-force" exercises to provide as realistic as possible an understanding of what terrorists might be expected to attempt to do. The assessments also frequently use sophisticated computer modeling tools, provide excellent insights into possible attack scenarios that could be employed and how those scenarios may be defeated by our protective forces. The various tools are then factored in to the preparation of a Site Safeguards and Security Plan (SSSP) for each nuclear site, a plan which helps the site manager understand how to employ the most effective protection strategy for his or her site.

During the course of the year various other forms of assessments are conducted at each site. They include self-assessments by the contractor operating the site to determine how the site is performing in each of the major areas of security. They include federal surveys or surveillances by NNSA federal staff to review how the contractor is performing. And they may also include Headquarters reviews by the Office of Independent Oversight and Performance Assurance (OA). The various reviews look at, among other things, protective force performance at each site against the threat scenarios expected for that site. They also include reviews of areas such as personnel security (the clearance process), information security, related to the protection of classified and sensitive information, and materials control and accountability, the management of nuclear

materials at each site. The result of these various reviews and assessments gives us an overall understanding of the situation at each sight.

Although Mr. Podonsky is testifying in more detail, I would like to speak briefly about the results of such reviews at NNSA sites over the last couple of years. Overall, the results of the most recent OA inspections have been positive, with the majority of areas reviewed being rated as "Providing Effective Performance." In some cases, areas were rated as "Needs Improvement." NNSA management is working to ensure that site managers remain focused on providing effective processes and making necessary improvements.

GAO

You have asked for my views on the draft GAO Report regarding the NNSA Safeguards and Security Program. As you know, the draft report provided four summary recommendations on areas where improvements could be made. These include: (1) defining clear roles and responsibilities for the NNSA headquarters and field site operations; (2) consistency in assessment of contractor security activities; (3) overseeing contractor's corrective action plans; and (4) allocating sufficient levels of federal staffing to site offices. I would like to address each of these recommendations.

Defining clear roles and responsibilities for the NNSA headquarters and field site operations

We have long recognized the need to clarify roles and responsibilities at NNSA, and we have done so. My predecessor, Administrator John Gordon, announced NNSA's strategy for improving effectiveness and efficiency in the February 25, 2002, ***Report to Congress on the Organization and Operations of the National Nuclear Security Administration.***

On December 19, 2002, I approved an organizational realignment standing up the new NNSA, creating eight Site Offices and one integrated Service Center, and disestablishing three Operations Offices. NNSA stood up a new organizational structure that: (1) removes a layer of management by disestablishing Operations Offices; (2) locates NNSA support and oversight close to the laboratories and plants by strengthening Site Offices; (3) consolidates support functions in a single Service Center organization; and (4) allows NNSA to adopt challenging staff reduction targets to be achieved by the end of Fiscal Year (FY) 2004.

NNSA's Site Office Managers have been designated the contracting officers responsible for integrating direction for the contractor. We further clarified safeguards and security roles and responsibilities by formally issuing the Functions, Responsibilities and Authorities Manual for safeguards and security functions in May 2003. GAO's report saw a snapshot from the old system, which we recognized as inadequate for the new, reengineered organization. We have made substantial progress, and we are heading in the right direction.

Consistency in Assessment of Contractor Security Activities

In its report, the GAO notes that reliance on surveillance is not consistent with DOE Orders calling for a comprehensive survey of a contractor's safeguards and security performance. NNSA has proposed language in the current revision to DOE Order 470.1, DOE O 470.1A, to include "Continuous Surveillance" as a recognized form of survey. In our efforts to improve processes, this is an example of getting ahead of the paperwork,

but having good intentions. We are taking a formal look at trends to ensure that the surveillance process we formalize will continue to meet the requirements.

Overseeing Contractor Corrective Action Plans

The GAO report noted that contractors have not consistently prepared corrective action plans to include formal, thorough, root cause analyses as called for in DOE policy and that the NNSA site offices had not identified such instances for correction by the contractor. The report also identified the need to assure that performance measures established for the contractor measure qualitative factors of contractor efforts wherever possible.

In late April, NNSA headquarters issued policy implementation guidance to its site offices to assure the thoroughness and documentation of corrective plan root cause and cost-benefit analyses. In addition, contractor performance of the safeguards and security program is an element of each of NNSA's annual contractor Performance Evaluation Plans (PEPs). The Plans are developed and owned by the Site Office Manager, who also serves as the site Contracting Officers and shares line management accountability for all operations at the site. The Site Office Managers develop the PEPs with input from the HQ program and staff offices. The performance measures addressing safeguards and security in the PEPs are generally qualitative in nature, and impact on the amount of fee that is earned. The Site Office Manager determines the level of contractor performance against the PEP, again with input from the HQ program and staff offices. The final annual performance ratings are approved by the NNSA Administrator who also makes the fee determination decision.

Allocating Sufficient Levels of Federal Staffing to Site Offices

We have looked carefully at the Site Office staffing levels and believe we have correct requirements for Federal staff. The current targets, issued in February 2003, were chosen to achieve the objectives of (1) performing the functions assigned in the Matrix of Functions and Activities by Location and (2) avoiding duplicating functions at Site Offices that could be performed as effectively at the Service Center or should be performed at Headquarters. Between February and August 2002, teams representing the future Site Offices and Service Center worked on developing a detailed matrix containing key functions and activities performed within the NNSA and assigning lead and participating roles to either the Sites, the Service Center and/or Headquarters. In October 2002, NNSA's senior leadership requested that Site Managers prepare staffing plans based upon assigned functions and workload. We held an NNSA staffing "summit" at the end of February 2003 in which each NNSA manager briefed his or her plan to the Leadership Coalition.

Safeguards and security is an important part of this NNSA effort. Where critical vacancies exist, hiring, support from the Service Center, other site offices and/or headquarters are all available options to assure each NNSA site has the appropriate skills mix to effectively execute their safeguards and security program assessment responsibilities. Finally, while the draft report references comments from the Department of Energy's Office of Independent Oversight and Performance Assurance regarding the potential to weaken security oversight if staffing and expertise at site offices are not addressed; they have also stated that NNSA's reorganization steps, to date, have helped to clarify roles and responsibilities for security oversight and that future plans have the potential to further strengthen security oversight.

Improvements/Management Challenges

Following release of the new Design Basis Threat (DBT) document in May, each NNSA site has been tasked to develop an implementation plan by this September. The new DBT will require each site to prepare a revised Site Safeguards and Security Plan, that outlines each site's protection strategies against our expanded threats. As a result, changes in operational procedures, materials and asset location, protective force deployment, application of technology and other efforts will be identified and factored into revised site SSSP's. Resources associated with any necessary changes will be identified from within existing or future budget requests.

The primary cause of NNSA's high Protective Force overtime rate and lack of time for Protective Force training is the increase in periods of elevated Security Condition consistent with raising the national threat level to Orange. The problem has been exacerbated by delays in the access authorization process for granting "Q" clearances to newly hired protective force personnel. A significant cause of the delay is the statutory requirement for all Security Police Officer clearances to be managed by the Federal Bureau of Investigation. Congress is considering an Administration proposal to give the Secretary of Energy more flexibility to refer some investigations to the Office of Personnel Management. The sites have begun to use the Accelerated Access Authorization Process; Headquarters has established a working group to streamline the DOE/NNSA process; the Albuquerque Service Center is now prioritizing clearances for FBI processing, on a site allocation basis. Progress is beginning to be made. As overtime is reduced, opportunities for training will increase.

The NNSA is continuing its efforts toward material consolidation. We have obligated funds to move, consolidate, or increase storage of nuclear materials at the Los Alamos National Laboratory, Sandia National Laboratory, and the Y-12 Plant. In concert with the consolidation effort are our efforts to integrate operational planning with security requirements. Two excellent examples are the Highly Enriched Uranium Manufacturing Facility at Oak Ridge and the proposed new Modern Pit Facility at the Savannah River Site. In both of these cases the Administration's security experts and operations personnel are working hand in hand to ensure that the new facilities can operate efficiently while maintaining required security. Though this approach requires a longer lead-time to address both sets of issues, the Administration believes this to be the correct approach.

Part of our approach in providing the required security discussed above is our pursuit of technology to enhance security while reducing potential jeopardy to our Protective Forces and reducing their associated long-term costs. Toward that end, beginning in FY 04 NNSA will pursue improvements in our ability to address Chemical and Biological threats; physical protection of Protective Forces; recapture and recovery of NNSA assets; improved detection and assessment; and complex wide access authorization data sharing. We will continue to assess and make changes to assure our physical security programs are effective and responsive to the evolving security challenges. This includes continued communication and sharing of issues, lessons learned and best practices and an emphasis on senior management involvement and accountability.

Design Basis Threat

I'd like to say a few words here about NNSA and the Design Basis Threat (DBT). This document identifies and characterizes potential adversary threats to selected Department nuclear weapons, components and facilities. We worked closely with the Office of Security in the development of the DBT that was issued last month. At no time during the NNSA evaluations or deliberations was budget a determining factor. The DBT by its own terms is a goal we are focusing on reaching. We are currently evaluating and will adjust the budget accordingly. It is premature to discuss the specific implementation or resultant costs at this time. We are working closely with the sites to develop cost-effective implementations plans in response to the requirements in the DBT.

Conclusion

In conclusion, I want to leave you with my assurance that I believe our nuclear complex security posture is strong. On going improvements are necessary both with respect to our facility protection posture, because the threat is always changing, but equally, as GAO has rightfully pointed out, our management of the nuclear safeguards and security program needs further improvement. I want to leave you with the assurance that the Secretary and I are personally committed to ensuring effective safeguards and security across all our operations. I would be pleased to answer any questions.

Mr. TURNER. Mr. Mahaley.

Mr. MAHALEY. Thank you.

Mr. Chairman, I appreciate this opportunity to provide the committee with information concerning the Department of Energy's recently completed efforts to update its design basis threat.

DOE recently revised its design basis threat policy to reflect changes in perceived threats to U.S. Government assets and operations. The new design basis threat policy, approved in May 2003, is designed to reflect the most credible threats to departmental assets and operations and provide a baseline for operational and budgetary planning purposes. The DOE design basis threat policy is derived from and associated with national intelligence threat information and other government agencies' threat policy statements.

The 2003 DOE policy is predicated on the information contained in the Defense Intelligence Agency, Postulated Threat: to U.S. Nuclear Weapons Facilities and Other Selected Strategic Facilities, dated January 2003, also referred to as the Postulated Threat Statement. The Postulated Threat Statement details relevant threat information about postulated adversary team sizes, characteristics, capabilities and applicability to national security assets. The Postulated Threat Statement is based on intelligence information detailing actual terrorist attacks and the equipment and tactics utilized in the attacks, expert judgments regarding stated terrorist intentions and their ability to execute the stated objectives and postulated capabilities based on the latest knowledge concerning terrorist activities.

Prior to September 11, prior to those attacks in New York and Washington, the Department of Energy in August 2001, requested that the intelligence community prepare an update to the 1994 Postulated Threat Statement. Although the 1994 Postulated Threat Statement was designed to be a 10-year document, we believed at that time the changes in international politics, emerging technologies and increases in worldwide terrorism required a reassessment. The National Intelligence Coordinating Committee assigned the primary responsibility for updating the Postulated Threat Statement to the Defense Intelligence Agency.

The events of September 11 delayed the Postulated Threat Statement update effort due to reallocation of critical assets. However, the requested Postulated Threat Statement update was fully underway by January 2002. The primary entities collaborating on the revision to the Postulated Threat Statement were the Defense Intelligence Agency, the Department of the Navy, Department of the Army, Department of the Air Force, Nuclear Regulatory Commission, the Federal Bureau of Investigation, the Central Intelligence Agency and the Department of Energy.

The Department of Energy's Office of Security, which I direct, began revising the DOE design basis threat policy in October 2001. Our work on the revised DOE design basis threat policy was carried out in parallel with the work on the updated Postulated Threat Statement to reduce the amount of time that would be required to issue a final DOE design basis threat upon completion of the Postulated Threat Statement.

After the release of the Postulated Threat Statement in January of this year, we made final revisions to the departmental design

basis threat policy; and the policy was then coordinated with the Department of Energy, including what Mr. Brooks has just pointed out, the National Nuclear Security Administration; and that revised policy was approved by Deputy Secretary of Energy Kyle McSlarrow on May 20.

The new design basis threat policy will provide managers an improved threat policy document to plan, resource and execute vital safeguards and security programs. In addition to updated threat information, the revised threat policy includes a significant enhancement over prior policies. We call it the use of a "graded threat concept." The graded threat concept considers and accounts for factors such as the consequences of a malevolent event, the attractiveness of the assets sought by the terrorists, the ability of an adversary to accomplish a given objective with an asset, and the resources required by an adversary to accomplish a given objective.

The graded threat approach includes the establishment of threat levels for departmental facilities and associated protection strategies based on the assets located at a given facility. The DBT, or design basis threat, policy separates the threat levels into two distinct categories. One category of threat levels covers threat, disruption of mission, espionage and foreign intelligence collection; and the second category of sabotage threat levels covers radiological, chemical and biological sabotage.

Five threat levels are established for theft, disruption of mission and espionage and foreign intelligence. Threat level one, which is the highest, are used to describe facilities that receive, use, process or transport or test what we call category IA assets. Those are nuclear weapons, nuclear test devices or completed nuclear assemblies.

The threat levels run through threat level 5, which is the lowest, for facilities that are only required to maintain minimum safeguards, accountability or security operations; and that is—an example would be a small office activity, a tenant in a larger office building or a small isolated research or test facility, facilities that don't possess quantities of special nuclear material.

Four sabotage threat levels are established for radiological, chemical and biological sabotage. Sabotage threat level 1—that is the highest level—through level 4, the lowest, are set for those facilities, buildings or operations that process, store or transport radiological, chemical and biological materials by the degree to which these materials, if dispersed, would result in acute dose effects at the site boundary.

Immediately following the events of September 11, the Department implemented measures to augment safeguards and security for the most critical Departmental assets. Ambassador Brooks described what happened in the NNSA. That was pretty much mirrored throughout the rest of the Department. Even our non-NNSA activities are sometimes involved in transporting nuclear materiel. Those shipments were suspended. We went to our highest possible security condition, absent—we went to SECON 2, is what we call it. SECON 1 is reserved for a situation where an actual attack is directed at a DOE facility. We went to our highest security levels, suspended shipments, and that was pretty much uniform throughout the Department.

The revised design basis threat policy is effective immediately and will be implemented over the next several years. Actions to augment existing safeguards and security programs for those facilities and assets that are considered the highest security priority will be undertaken as soon as practicable.

Mr. Chairman, that concludes my prepared testimony. Thanks for the opportunity to appear before the committee, and I'll be happy to answer questions.

Mr. TURNER. Thank you, Mr. Mahaley.

[The prepared statement of Mr. Mahaley follows:]

STATEMENT OF

JOSEPH S. MAHALEY

DIRECTOR, OFFICE OF SECURITY

DEPARTMENT OF ENERGY

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND

INTERNATIONAL RELATIONS

COMMITTEE ON GOVERNMENT REFORM

U. S. HOUSE OF REPRESENTATIVES

JUNE 24, 2003

Thank you, Mr. Chairman, I appreciate this opportunity to provide the committee with information concerning the Department of Energy's recently completed efforts to update its Design Basis Threat.

The Department of Energy (DOE) recently revised its Design Basis Threat Policy in 2003 to reflect changes in perceived threats to United States government assets and operations. The new Design Basis Threat Policy, approved in May 2003, is designed to reflect the most credible threats to Departmental assets and operations and provide a baseline for operational and budgetary planning purposes. The DOE Design Basis Threat Policy is derived from and associated with national intelligence threat information and other government agencies' threat policy statements.

The 2003 DOE Design Basis Threat Policy is predicated on the information contained in the Defense Intelligence Agency, "Postulated Threat: to U.S. Nuclear Weapons Facilities and other Selected Strategic Facilities," dated January 2003, also referred to as the Postulated Threat Statement. The Postulated Threat Statement details relevant threat information about postulated adversary team sizes, characteristics, capabilities and applicability to national security assets. The Postulated Threat Statement is based on intelligence information detailing actual terrorist attacks and the equipment and tactics utilized in the attacks, expert judgments regarding stated terrorist intentions and the ability of the terrorist to execute the stated objectives, and postulated capabilities based on the latest knowledge concerning terrorist activities.

Prior to the September 11, 2001, attacks in New York and Washington, the Department of Energy, in August 2001, requested that the intelligence community prepare an update to the 1994 Postulated Threat Statement. Although the 1994 Postulated Threat Statement was designed to be a 10-year document, we believed at that time that changes in international politics, emerging technologies and increases in worldwide terrorism required a reassessment. The National Intelligence Coordinating Committee assigned the primary responsibility for updating the Postulated Threat Statement to the Defense Intelligence Agency.

The events of September 11, 2001, delayed the Postulated Threat Statement update effort due to reallocation of critical assets. However, the requested Postulated Threat Statement update was fully underway by January 2002. The primary entities collaborating on the revision to the Postulated Threat Statement were: the Defense Intelligence Agency, the Department of the Navy, the Department of the Army, the Department of the Air Force, the Nuclear Regulatory Commission, the Federal Bureau of Investigation, the Central Intelligence Agency, and the Department of Energy.

The Department of Energy's Office of Security began revising the DOE Design Basis Threat Policy in October 2001. Our work on the revised DOE Design Basis Threat Policy was carried out in parallel with the work on the updated Postulated Threat Statement to reduce the amount of time that would be required to issue a final DOE Design Basis Threat Policy upon completion of the Postulated Threat Statement. After the release of the final Postulated Threat Statement in January 2003, we made final revisions to the Departmental Design Basis Threat Policy. The

Policy was then coordinated within the Department of Energy, including the National Nuclear Security Administration. The revised Policy was approved by the Deputy Secretary of Energy on May 20, 2003.

The new Design Basis Threat Policy will provide managers an improved threat policy document to plan, resource, and execute vital safeguards and security programs. In addition to updated threat information, the revised Design Basis Threat Policy includes a significant enhancement over prior policies - the use of the "graded threat concept". The graded threat concept considers and accounts for factors such as consequences of a malevolent event, the attractiveness of the asset, the ability of an adversary to accomplish a given objective with an asset, and the resources required by an adversary to accomplish a given objective.

The graded threat approach includes the establishment of "Threat Levels" for Departmental facilities and associated "Protection Strategies" based on the assets located at a given facility. The Design Basis Threat Policy separates "Threat Levels" into two distinct categories. One category of "Threat Levels" covers theft, disruption of mission, and espionage and foreign intelligence collection, and the second category - of "Sabotage Threat Levels" - covers radiological, chemical, and biological sabotage.

Five "Threat Levels" are established for theft, disruption of mission, and espionage and foreign intelligence collection: Threat Level 1 (the highest) – for facilities that receive, use, process, store, transport, or test Category IA assets (i.e., nuclear weapons, nuclear test devices, or completed nuclear assemblies) through Threat Level 5 (the lowest) – for facilities that are only

required to maintain minimum safeguards accountability or security operations (i.e., small office activities, tenants in large office buildings, or small isolated research or test facilities that do not possess quantities of special nuclear material).

Four "Sabotage Threat Levels" are established for radiological, chemical, and biological sabotage. Sabotage Threat Level 1 (the highest) through Level 4 (the lowest) are set for facilities, buildings, or operations that process, store or transport radiological, chemical, and biological materials by the degree to which these materials, if dispersed, would result in acute dose effects at the site boundary.

Immediately following the events of September 11, 2001, the Department implemented measures to augment safeguards and security for the most critical Departmental assets. The recently revised Department of Energy Design Basis Threat Policy incorporates those measures and, in some cases, sets a higher standard for the protection of Departmental assets.

The revised Design Basis Threat Policy is effective immediately and will be implemented over the next several years. Actions to augment existing safeguards and security programs for those facilities and assets that are considered the highest security policy will be undertaken as soon as practicable.

That concludes my prepared testimony. Thank you for the opportunity to appear before the Committee. I'll be happy to answer questions.

Mr. TURNER. We want to recognize Mr. Todd Platts from Pennsylvania has joined us for the hearing, and welcome.

Also, I ask unanimous consent to insert into the hearing record at this point a statement from Senator Charles Grassley of Iowa. Senator Grassley is a co-requester with the subcommittee on related GAO work that will be the subject of a future hearing.

[The prepared statement of Senator Grassley follows:]

UNITED STATES SENATOR • IOWA
CHUCK GRASSLEY

http://grassley.senate.gov
grassley_press@grassley.senate.gov

Contact: Jill Kozeny, 202/224-1308
Beth Pellett, 202/224-6197
Dustin Vande Hoef, 202/224-0484

Statement of Sen. Chuck Grassley, of Iowa
Subcommittee on National Security, Veterans Affairs
And International Relations
Committee on Government Reform
U.S. House of Representatives
"Our Nuclear Weapons Labs: In Harm's Way"
June 24, 2003

Thanks to your outstanding leadership on oversight, Mr. Chairman, this important hearing is taking place today. I am honored to be a part of it. I thank you for allowing me to testify. And I thank you from the bottom of my heart for your continuing interest and commitment to oversight and investigation or O&I.

O&I is an essential part of what we do here in Congress. Putting the public spotlight on ugly problems is the heart and soul of oversight. Today we are going to shine the public spotlight on lab security.

The labs are in harm's way. Security is lax. Our nuclear secrets are not safe. The labs are R&D facilities for weapons grade materials, weapons reactors, weapons design and test data as well as other highly classified information pertaining to those programs. These critical commodities are sought by foreign governments and terrorist organizations bent on acquiring weapons of mass destruction.

Mr. Chairman, I just don't get it.

The labs contain some of the most sensitive and the most sought after technology in the world today. This stuff should be locked up tight like at Fort Knox and guarded night and day by alert sentries.

To criminals and spies, the labs must be like a candy store with the front door left wide open and nobody at the register. And the terrorists must be licking their chops.

Without swift and decisive corrective action, a lab could easily be converted to a very dirty bomb and blown up in our face. This situation is totally unacceptable.

Mr. Chairman, I hope we can work together and keep the public spotlight focused on the problem until we create enough pressure to get it fixed.

I am new to this inquiry. You, by comparison, have had the General Accounting Office (GAO) working on lab security since October 2001. We didn't officially team up until May 22, 2003 when we co-signed a letter to the GAO. We directed the GAO to expand its ongoing investigation to address a broader range of issues, including management oversight of internal security investigations.

Mr. Chairman, I didn't intend to get involved in lab security. I was drawn to it by necessity.

Over the past 8 months, 5 whistleblowers from two labs have come to my office with a laundry list of horror stories. Four of the whistleblowers were fraud, waste, and abuse investigators; one was Operations Chief of the Protective Force.

All have been threatened with reprisals and removed from their jobs for committing truth. The information they have given me is compelling. I could not turn my back on these brave soldiers for the truth. I had to get involved and help.

Once the information began pouring into my office, I started writing letters to Secretary Abraham. So far I have sent him five letters. My letters to Secretary Abraham summarize the most egregious allegations. There is a list of 102 different security investigations. These were conducted between 1997 and 2003.

For the most part, these are aborted investigations - investigations that went no where because of orders from above.

I will now take a moment to highlight the most egregious cases I know about. These are as follows:

–Several "Little Boy" atomic bombs on public display in museums, including the Smithsonian, contained secret restricted data;

–An FBI surveillance operation captured at least a dozen members of the security force engaging in misconduct on video tape, including sleeping on duty; Members of protective force can earn up to $110,000.00 a year with overtime; At that price, they should stay awake;

–A member of the guard force was caught on FBI video tape stealing computer components; and later sold them to supervisors at below market prices;

–Sensitive facilities - like inside the reactor area - and the SCIF [Sensitive Compartmented Information Facility] are left unlocked and/or unalarmed at night;

–Activated alarms in highly secure areas trigger no response; Guards simply re-set alarm circuits in command center and make no attempt to investigate possible intrusions; An evaluator performed jumping jacks in a nuclear reactor area to activate alarms and test guard response, but there was no guard response;

–A classified hard drive containing weapons research data is missing from a vault;

–Master keys providing access for everything right up to the glass doors of the reactors - "went" missing from guard force custody at two labs; Locks never re-keyed at one lab;

–The same security gate turnstyles costing $25,000.00 each were repeatedly sold to the lab for $50,000.00 each, netting $3 million in cash to cover excessive guard force overtime;

–Vice President David Nokes allegedly ordered the destruction of a hard drive that is critical evidence in an ongoing investigation of gross misconduct in the highly classified "5900" area SCIF; The hard drive was first destroyed with a magnet and then a sledge hammer; the hard drive allegedly held nude photos involving two employees - [----]; the photos were taken with a digital video camera brought into the SCIF area without clearance or authorization; [----] is described as "con man and professional computer hacker;" He established unauthorized computer links in and out of SCIF and is known to have planted an unauthorized intercept-type software - called Spector Key Key - in some management computers;

-A Verizon maintenance van parked inside a classified area was stolen at 5am and crashed through perimeter fences in what is characterized as a "high risk" exit; The van was discovered in the parking lot of a nearby Home Depot store; There are no clues as to why the van was stolen, but its theft coincides with the disappearance of a classified Sun computer system from the SCIF; Investigators were unable to check alarm data because protective force radio and telephone recording system was turned off;

–FBI sting operation recovered large numbers of stolen lab lap tops and CIA computers from Doctor Dan's chop shop in Albuquerque; computers are stripped of serial numbers, chopped up and re-sold; computer losses at one lab are estimated at $700,000.00 per year; the prime suspect - [----] - is still employed at the lab;

–And now there is plutonium missing at Los Alamos

There is a very disturbing pattern that cuts across all of these aborted investigations. I call it the common denominator. It is buried in the culture. It tempers management's response to every security problem. It is an attitude - a state of mind. And it's really bad news.

The culture stands in the way of accountability, corrective action, and effective security. It is the single most significant problem at the labs.

The typical management M.O. at the labs works something like this: Quash the investigation; Sweep it under the rug - fast; And shoot the messenger. One source says the lab M.O. is: "deny everything and make counter accusations." Revelations about security breaches are an embarrassment to the lab. They are suppressed at all costs and never reported up the chain of command.

Mr. Chairman, if you have doubts about the existence of the culture today, just check lab Vice President Don Blanton's All-Hands video address on April 16th. I have it right here in my hand.

Mr. Blanton trashes the whistleblowers who came to my office when they were unable to get their concerns about security addressed internally. He trashes them in front of the whole department.

And he trashes the whistleblowers after the lab President, Paul Robinson, had publicly praised them for having the courage to "bring these issues forward by other means" - that is, directly to Chuck Grassley.

When his derogatory remarks leaked out, Mr. Blanton was forced to make a public apology on May 9th. Mr. Chairman, if you think we have seen the last quashed lab investigation, I have news for you. There appears to be more cover-up work in progress right now - today.

I am talking about the Bay Report completed on June 4th. It's 80 to 90 percent pure whitewash. The Bay Report is supposed to be an independent look at the aborted security investigations.

It examined five of the most egregious cases and concluded that only one of five "was clearly obstructed or impeded." The rest are fine. I don't buy it. The Bay Report does not say one word about lab security.

It is a personnel report on two whistleblowers. It concludes that there was no real retaliation - only the "appearance of retaliation." If it looks and smells like retaliation, it is retaliation. I fear that management will now use the Bay Report to broom the whistleblowers into the dustbin of history.

In this environment, there is no incentive to connect the dots. Dots are key pieces of information investigators must connect to solve crimes - like putting a puzzle together.

Focusing on one dot is the specialty of lab managers. For instance, according to sham lab reports, the missing set of master keys was mere carelessness. They were inadvertently left in someone's gym bag and forgotten for 11 days - even though computers are disappearing right and left with no evidence of forced entry.

The stolen Verizon Van was written up as routine auto theft.

Nude photos taken with an unauthorized camera and downloaded on to a hard drive in the SCIF was nothing more than run of the mill employee misconduct.

To current management, the van stolen from a classified compound crashing through perimeter fences at 5am is mickey mouse stuff - pranks.

Lab President, Mr. Paul Robinson, characterizes some of these issues as "monkey business." A management team that has a healthy respect for security would assume that the master keys could have been taken in the furtherance of some other crime - like theft of government property - or theft of sensitive information - or even espionage.

The nude photography that surfaced on the hard drive in the SCIF could have been part of an elaborate scheme to conceal espionage activity. It could have been a clever distraction operation. An unauthorized camera in or near the SCIF is a red flag.

What about the illegal intercept software that was planted in all the labs' computers by a person known to have suspicious connections? Two years have passed, and it still hasn't been checked out. Why?

The Cox report makes it crystal clear that our nuclear weapons labs - Los Alamos, Lawrence Livermore, Oak Ridge, and Sandia - are targets for China's "long-term, ongoing intelligence collection effort." The Cox report is a wake-up call - if I ever heard one.

Management needs to start thinking "outside the box." Management needs to start considering worst case scenarios and react accordingly.

When Sandia's authorities learned about the missing keys, for example, a counter-intelligence sweep should have been conducted for "bugs" in sensitive areas. None was conducted.

The alarm data should have been analyzed for unexplained intrusions in sensitive areas. None was conducted.

Why wasn't the alarm data for the night the van was stolen checked for unexplained intrusions? Everything I read in the newspapers tells me that foreign agents are already inside the labs.

The Cox report warned us they were coming and that they would keep coming. I think we have to assume they are there. We have identified some of these agents, but there must be others we don't know about.

When the presence of foreign agents is coupled with missing keys for every lock at two labs; and unauthorized photography is going on in the lab's most sensitive area, the SCIF; and a van is stolen from a classified area at 5am and crashes through perimeter fences and coincidentally a classified computer is missing from the SCIF; and top management calls it "monkey business," I fear the worst.

There are gaping holes in the security net, and we don't know where they are. Security breaches at our nuclear weapons labs is nothing new, Mr. Chairman. It's an old story.

Four years ago, the Rudman report recommended the creation of a semi-autonomous agency to address the problem. That led to the creation of the National Nuclear Security Administration - NNSA.

NNSA is supposed to be THE FINAL ANSWER. Its primary mission is to tighten security at the labs. But I am not sure that any of the 2,391 NNSA employees know it. The NNSA mission statement doesn't say it.

Everything I see and hear tells me that we are right back at square one. All we succeeded in doing by creating NNSA is to rearrange the chairs on the deck of the Titanic. You can't put a fancy saddle on a mule and call it a race horse.

We are still stuck with ineffective management oversight of the labs. Secretary Abraham needs to take charge.

The culture is the root cause of the problem. The culture must go. And since the culture lies in the hearts and minds of the top managers, maybe that's where reform needs to begin. For example, if lab Vice President David Nokes obstructed an investigation by ordering the destruction of evidence as confirmed by authoritative sources, then his head should be the first one to roll.

The Inspector General (IG) should step in and help Mr. Abraham root out the problem. But as I see it, the Energy Department IG is AWOL on lab security. One senior official put it this way: "the IG just dabbles in it," and that's a direct quote.

The Director of the Office of Independent Oversight, Mr. Glenn Podonsky, is doing an excellent job. He is the one who jumped in and said the lab's preliminary response to my questions was "less than adequate." That's a reference to the "Wisdom Report" that summarily dismissed the allegations raised in my letters as "unsupported by evidence."

I thank Mr. Podonsky for his honesty in setting the record straight. Unfortunately, he is looking at the problem through a straw - seeing each lab as an isolated case - instead of taking a global view. If Mr. Podonsky could step back and take in the big picture, he would see definite patterns in the security failures across-the-board at all the labs.

Since Mr. Podonsky first came to my office to address issues at Sandia - when Los Alamos was fresh in our memories - we have witnessed a melt down at Lawrence Livermore. The lab's trusted security chief was involved with a Chinese double agent; the lab lost a set of master keys along with an electronic Tesa key.

These security breaches led to Mr. Podonsky's extended visit at Lawrence Livermore. I suspect that Mr. Podonsky is now coming around to my way of thinking. He's thinking globally.

Somebody at the very top, who can wrap their arms around all the labs and clearly see the whole problem in its totality, must take charge. That person needs to get the reform process jump started. It's time for everyone involved to stop wringing our hands in frustration and do something bold.

Mr. Abraham is the man at the top. "The buck stops here," as Mr. Truman used to say. In a meeting on April 7th, Secretary Abraham convinced me he is committed to doing what must be done. Secretary Abraham now needs to order his top deputies to tighten the noose on security at the labs. The top deputies need to issue firm guidance that clearly sets the standards for lab security.

Thank you for your patience, Mr. Chairman. That concludes my statement.

Mr. TURNER. Mr. Ambassador, I appreciate your comments and the confidence in which you describe the actions that you're taking. This is obviously—when you start hearing some of the testimony about procedures and processes, it certainly loses some of the excitement I think we all would expect in the severity of the issue that we're dealing with, which is the security of our nuclear facilities and really the catastrophic consequences if you don't succeed.

We've had testimony from the General Accounting Office; and we know that even the NNSA has indicated that they're—you are concerned that, at times, that managing the safeguards and the security programs have not been fully effective and the concerns as to the security of the complex.

In listening, Ambassador, to the actions that you're taking, clearly you've acknowledged some problems that have occurred in the past, that you've not been fully satisfied. I'm assuming that you're not fully satisfied still as to where you are as a result of your actions, but I guess the big question that I have is, you know, what do you need? In addition to the authority that you have and the actions that you're taking, what do you see as you survey what the problem is in front of you that you currently don't have, either in authority or resources?

Mr. BROOKS. I believe that I largely have the authority and the resources I need.

There are specific, once again, lower-level issues. For example, we have asked the Congress to change the law to allow investigations of some of our people to be conducted by the Office of Personnel Management rather than the FBI. If you look—we are not able to discern any difference in the quality of the OPM/FBI investigations, but we have to have them done before we can give them the appropriate clearance to be in sensitive facilities, and that includes guard force.

What we are able to discern is that the waiting period for the FBI is sort of in the mid-200 days, and the waiting period for OPM investigations is in the range of 180 days. So we have asked the Congress to give the Secretary the flexibility to direct our investigations to the OPM.

Now, this sounds like a very technical point, but it's not. It's not because the first line of defense is the guard force, but you can only use guards where appropriately cleared, and nobody wants to change that. And so, as you try to expand your guard force, you—it is important to be able to move rapidly to get them cleared. That is particularly true since one of the problems that we are working on is that our guard forces generally are doing a lot of overtime.

Now, if you talk privately to the guards, they tend to like overtime, at least some of it, because they actually base their standard of living on the assumption that they're going to get some overtime. But we're doing more of it than we'd like to do.

One problem, for example, has been each time the Nation goes to Homeland Security level orange, Mr. Mahaley and I tell the Secretary he should go to SECON 2, and he does. What that does is put more guards around things; and since there aren't any more guards, what it means is people work longer hours.

So anything I can do to speed up the process of bringing on new guards at these plants is a useful thing, but that's not a very pro-

found thing. It's illustrative in my view of the fact that security is a whole lot of individually not very glamorous things carried out day in and day out. But I'm not here saying, oh, if only the Congress would give me more money. I could certainly think of things to do with more money. This is not primarily a money problem. This is a roles-responsibilities-oversight culture problem that we're trying to solve right now.

Mr. TURNER. I take it, though, that you do remain concerned as to the performance level. The initial question is your level of satisfaction—you're saying that you have the authority and the resources, which is a great the-buck-stops-here answer, and I wanted to get a sense from you that you do have some concern and that this is not——

Mr. BROOKS. I do have some.

Mr. TURNER [continuing]. Happening in a timely manner and it is not happening as effectively as it should.

Mr. BROOKS. Sir, we're dealing with nuclear weapons. You've got to be concerned at anything less than perfection. So of course I'm concerned.

On the other hand, I think that we are moving in the right direction. I think that the—as you heard from Mr. Podonsky, there have been some substantial improvements.

I think that where I have, for example, cultural problems, cultures don't change overnight. All right? If you have problems of being lax in enforcing rules, if you have problems of not being prompt in reporting problems, those are cultural problems and training problems, and you change them, but it takes time.

So I don't want to mislead the committee. I think I'm headed in the right direction. I think I'm seized with a problem, but I don't think if you invite me back in 2 weeks I'm going to be able to walk in and say look at the wonderful things we've done in the last 2 weeks. I don't think that is the way this problem works.

Mr. TURNER. Thank you, Ambassador.

Mr. Tierney.

Mr. TIERNEY. Thank you, Mr. Chairman. Mr. Ambassador, Mr. Mahaley, thanks for joining us.

Mr. Ambassador, I think you were correct in saying that most of these things go back to management. I know the Secretary had made a statement that he was going to take the University of California—the contract, put it up for review. It expires in 2005. Are you mindful that is the correct way to proceed? And if you are, should something be done between now and 2005 to enhance the job that we think they're doing?

Mr. BROOKS. Well, since the Secretary made that decision based on a recommendation from the Deputy Secretary and me, I certainly support it. We are doing things, not so much pointed in 2005, because we're doing things to continue to improve. The problems at Los Alamos that led to that decision did not spill over into security. They were primarily in business services, although you've recently seen one example that may spill over into security. There was what appears to have been a bookkeeping problem associated with a very small amount of plutonium. The best I can tell, that problem, which happened 2 years ago but was only recently discovered, is another example of a general lax approach to business

processes and the first one that actually spills over and has security things.

One of the reasons that we were so concerned was the fear that poor discipline in processes in one area sooner or later spreads. So while I don't mean to minimize the importance of control of term and wise stewardship of the public money, you want to stomp out the problems in that area before they get to things like classified material control or physical security.

What is being done in Los Alamos is the new laboratory director, who was put in with our approval by the University following the problems, is doing a major top-to-bottom overhaul of his business processes. So I don't think there's anything that needs to be done between now and 2005 that is not being done.

Mr. TIERNEY. On the oversight issue—either of you gentlemen or both of you might want to respond to this—the assertion is made that some of the reviews of the test of the performance of the security were being dumbed down. Can you talk about that a little bit, give us some assurances to——

Mr. BROOKS. I think you—Mr. Podonsky, in the previous panel said that he believes that is an accurate description of the way it was in the 1990's, and he doesn't believe it is an accurate description of the way it is now.

Mr. TIERNEY. Are you comfortable that it's not?

Mr. BROOKS. I am comfortable with that.

Mr. TIERNEY. The fact of the matter is that terrorists now appear ready to give up their own lives in order to accomplish their purpose. So it becomes pretty important for us not just to worry about containing them once they get to site but keeping them out of that site. Are you mindful of the fact or do you feel confident of the fact that all NNSA facilities are able to do that at this time?

Mr. BROOKS. Yes.

Mr. TIERNEY. And what do you base that on?

Mr. BROOKS. I base that on a series of reviews by Mr. Podonsky, a series of reviews by me and then an approach that my predecessor started called "Iterative Site Analyses," which is another way of looking at the design basis threat that Mr. Mahaley was talking about as the standard against which we try and make that assessment.

I don't yet know whether or not I can make that statement about the May 30th design basis threat or what I have to do to be able to make that statement. I don't mean to get into details in an open session. At most of my sites, I'm pretty comfortable that I was ahead of the new design basis threat at. At one or two sites, there may be one or two things we're going to need to do; and we're still looking at that.

Mr. TIERNEY. Well, I'm going to let you go with that, because my next question I think will take us into the closed session this afternoon about what level of comfort Americans should have generally about all of these sites. But given the fact that the design basis threat is just evolving and you've got to make some assessments on that, I'll yield back the balance of my time. Thank you for your answers.

Mr. TURNER. Mr. Chairman.

Mr. SHAYS. Thank you.

Mr. Brooks, I found both your testimonies helpful, but I was particularly interested in your testimony given that it—your oral testimony had an action plan that was not part of your written testimony. I inquired if maybe that was written down, and it wasn't. Could you go through your action plan.

Mr. BROOKS. Sure. I actually had hoped to be able to hand you a press release today. I actually think I'll now be able to hand you a press release tomorrow because of a teeny, tiny internal——

Mr. SHAYS. It's not a criticism. I'm delighted to——

Mr. BROOKS. But what I'm doing first, we are going to augment drawing from a number of things. We're going to make use of some of Mr. Mahaley's people. I'm going to make use of some contractor people. I'm going to make use of other people. I'm going to at least temporarily beef up the number of people that I have working on this issue.

Second, I'm going to use those beefed-up people and use my sites to be more vigorous on safety and—safeguards and security, but also to be reporting more directly to me. And, frankly, that's symbolic. I don't want to pretend that I know as much about safeguards and security as the superb people I have working for me or the superb people Mr. Mahaley has working for him, but it is my experience that when you have to report to the senior person then there could be no question that this is something that you take seriously.

Third, we have been the subject of a number of external reviews, most of them critical. By "we," here I mean the whole Department as well as the NNSA over the past several years. We're in the process of systematically going through all of those, looking at their recommendations, seeing whether we implemented them and then, if we didn't, looking again to see whether or not we should. I don't want to have a situation in which people thought that a problem was going to be solved without X or Y.

And, fourth, I'm asking Admiral Rich Mies to look specifically at physical security throughout my complex, and I'm going to—while not limiting him, I'm going to ask him to be very specific about one or two ideas that periodically flowed around about better management.

And, finally, as we have in the last month or two been looking at this problem, I have become concerned about people. I'm not sure I completely agree with the GAO that I'm short now, but I'm real sure that if I don't take aggressive action now, I will be short in terms of quality and experience in the future. The last time we had that problem was on weapons designers, and we got Admiral Chiles to run a commission to look at how we ensured that we had a stable corps of weapons designers. I'm asking him to do the same thing for safeguards and security professionals.

So that's the five things I'm doing.

Mr. SHAYS. I know I'm being redundant, but—before I'm redundant, let me ask another question. You said you agreed with all but one of the four major——

Mr. BROOKS. Yes, sir.

Mr. SHAYS [continuing]. Categories. And the one—defining clear roles and responsibilities, there was assessment, site security activities. That is the one you disagreed with.

Mr. BROOKS. The method of surveillance versus surveys is the method—it's actually their second or third. I can't remember. I'll have to look at the—I don't have the—let me just look at the——

Mr. SHAYS. But the other one, overseeing contractor, corrective actions and the others, allocating staff. But the thing I thought was interesting, though, was you seem to disagree with defining clear roles and responsibilities because——

Mr. BROOKS. Well, no, sir. I didn't mean to say that. I'm sorry. The defining clear roles and responsibilities is the precursor to everything.

Mr. SHAYS. I think you jumped in too quick. You may want to let me finish.

I was very impressed with your testimony, and I was encouraged by it, but I was—you said you would challenge anyone to check with people along the chain about their not knowing what their roles and responsibilities were, and so I think that's what you said, and that seemed to be suggesting that you were disagreeing with the GAO's findings that there wasn't this—so I must have missed something here.

Mr. BROOKS. I wasn't precise. Let me try again.

The GAO conducted their audit over a very lengthy period of time. Many of their interviews with individual sites were conducted 18 months ago. In response to a question I think from you, the GAO used the illustration that, when they went to individual sites, they said we don't quite know who's supposed to do what, so we're deciding on our own.

I believe that part of the problem I have corrected with the reorganization announced in December and the promulgation of formal roles and responsibilities. And I agree completely with the GAO's assessment that the problem is important. I believe I have done a great deal to correct it, and I'm going to continue to push that. That's what I was trying to convey, sir.

Mr. SHAYS. Thank you.

Mr. TURNER. Mr. Ruppersberger.

Mr. RUPPERSBERGER. I'm glad the issue has been raised about it starts at the top in management; and, again, I was impressed with where you're going.

Now, the one thing is to have a plan. The other thing is to implement a plan.

No. 1, how is your relationship and working relationship with the intelligence agencies—the CIA, FBI, whatever—as it relates to the security of the plants? I mean, are you working closely with them? Could you just—what you can say in this open hearing? Where are you with respect to that relationship? Because it seems to me one of the—the No. 1 component to deal with the issue of terrorism is the issue of intelligence.

Mr. BROOKS. Sure. The Department of Energy's Office of Intelligence reports to the Secretary, but I am, if not their largest customer, certainly their most eager customer. I am briefed by the intelligence agencies daily. I look at specific details of threats daily. As you know from the open-source accounts, there's a lot of chaff in that wheat, but we look carefully daily. When I see something that I believe requires us to pay attention, I make sure that it gets to my site managers and my contractors.

My sites also have field intelligence elements. They focus in two directions. One is the national labs, actually which is where a good deal of our technical intelligence on nuclear weapons is done; but, second, they provide another mechanism for disseminating things out.

There's probably no area in which I am more comfortable than that I'm fully plugged into the intelligence community and getting what I need. The problem of course, as September 11 taught us, is that we cannot depend solely on the hope that the intelligence community will discover problems.

But I know what the intelligence community knows. I'm fully comfortable. I suspect that's true for Mr. Mahaley also, but he should speak on that.

Mr. MAHALEY. Sir, I've seen a big change since September 11. DOE's Office of Intelligence has been—in the past—I've been there awhile. This is my 7th year as head of security, and the Office of Intelligence was traditionally directed at nonproliferation, looking at information collected around the world and advising, sort of being the government's lead analysis center on that intelligence as it regards nonproliferation and nuclear weapons development.

Since September 11, the Office of Intelligence has focused—and it was at my request in terms of I wanted a counterterrorism focus to try to pull together the information from all the agencies. Because, you know, we can beat these people. It's just what we've got to talk to each other and share the information. So the new director of intelligence has elevated the counterterrorism section to a division, and the director of that division reports to me at least once a week with a detailed analysis of everything he's covered in the previous week. Some days I get briefed two or three times a day.

Mr. RUPPERSBERGER. Well, that's good. And the teamwork—I think if you look at what's happened since September 11, the teamwork with all of our agencies, which in the past hasn't been as good, has helped to deter another incident.

Let me get to the issue of your security now with respect to your contractors. You have a large amount of contractors that deal with your security. Do you feel secure that your oversight of these contractors—that they are doing the job, that they're assessing themselves? I mean, are there any checks and balances there to make sure that there's consistency because you have different sites throughout the country? My concern would be, is—and another issue, you have three different components, I guess, in your operation. Is that too much bureaucracy, or would you feel more comfortable probably not to Federalize as it relates to this entire issue instead of the contractors that we have right now?

Mr. BROOKS. Let me—first, one reason that I'm comfortable that I know across the organization what is going on is the ability to use Mr. Podonsky's organization, the Office of Independent Oversight Performance Assurance. They look at all the sites, and therefore they are able both in a formal and—what's even more important—in an informal way to tell me whether there is consistency in approach.

An example is the Secretary and I have asked him to look at protective forces throughout the complex, because we've had problems now at two of our sites in which individual protective force officers

found problems and they weren't promptly reported. We're trying to understand whether those are unique problems or broad problems, and so we're going to look at protective forces throughout the sites.

With regard to Federalization of security, the problem there is I think manpower and whether or not you are likely to be able to come up with a sufficient Federal force and have the needed flexibility. It's one of the things I want these two groups I've chartered to look at, but my biases are that the problems that we are having is not because the force is not Federalized.

Now, there is one component that is. The Office of Secure Transportation, the people who actually move plutonium from here to there or weapons from here to there, that's an entirely—those are all Federal agents.

As far as Federalizing the entire contractor—the force—I think the country made a decision a long time ago that the national labs in particular but the plants, too, weren't the sort of thing that the Federal Government ought to be directly operating. I tend to agree with that. I can go into more detail if you need, but I certainly would not think that Federal control of the internal workings of the labs and plants will make anything better. Federal control of security is an idea that comes up and needs to be taken seriously. I personally think it will just change the problem. I don't think it will improve it.

Mr. RUPPERSBERGER. All right. Thank you.

Mr. TURNER. Mr. Platts.

Mr. PLATTS. Thank you, Mr. Chairman.

I apologize. I need to run off, but I do appreciate your testimony and the written testimonies you provided.

Just one question before I go is the—appreciating the focus on the management and the defined roles and increased security staff numbers, but one of the things that jumps out to me in the GAO report is that, in relation to the new design basis threat, that the GAO estimates that it will probably be the 2006 fiscal year before we really get a full picture of what the cost of the changes are going to be required in relation to meeting this new design basis threat and anywhere from 2 to 5 years till we fully implement and have these new procedures in place and really do what we want them to do.

My question is, do you agree with this general timeframe that GAO predicts? And, if so, what is the greatest reason for that time—that delay, given the seriousness of the threats we're talking about? This is saying really anywhere from maybe another 6 to 8 years, and you reference in your opening statement about not wanting a successor to be sitting here in 10 years having to answer similar questions. My worry is that, you know, 6 to 8 years from now the threat again will be different and we'll be always playing catch-up. So do you agree with it? And why is it going to take so long to get implemented? What is the greatest challenge in getting this done?

Mr. BROOKS. I agree that we're going to phase things in. I think the time lines that you cite are probably wrong. I expect to know what this is going to cost by early fall so that we can adjust the

fiscal year 2005 budget, which is the next one we get to prepare, as necessary.

The design basis threat document—and we'll have Mr. Mahaley comment further, if he would—is in fact—if you have something that you can meet in a day and a half, you haven't looked rigorously enough. We have looked—Mr. Mahaley in particular has looked at the changes that we have to think about because of the changed realization of the degree of organization that terrorists might have, and so we're basically taking a step to improve, and that takes time.

I am not quite sure where 6 to 8 years comes from. That's certainly not my understanding of my guidance from the Secretary, and I don't believe that's what the promulgation for the new document says.

Mr. PLATTS. If you have a good handle on the costs associated with the changes necessary by this fall, you're into the beginning of the 2004 although we may not, depending on how fast the appropriations bill—we may not yet have an 2004 appropriations done.

Is there consideration being given at this point to coming forward with a supplemental request because of the seriousness of the issues we're talking about, and that rather than waiting for the 2005 budget, to get it in there and have to go through the process, that we look at 2004 and say, here's what we now know we need; we don't want to wait a year because of the threat that we're talking about? Is that something under consideration?

Mr. BROOKS. I think it's premature to know the answer to that. I mean, my initial impression is that I'm not talking—on my side of the house; I can't speak for the rest of the Department—that I'm not talking, at most of my sites, about significant funding and that I—that a supplemental would not be appropriate. The decision to submit supplementals is not one that Mr. Mahaley and I get to make.

I will simply say that if——

Mr. PLATTS. But recommendations as to——

Mr. BROOKS. If I believe that I have a problem, the Secretary has made it fairly clear that he wants to hear about it. But at the moment I don't know—I do not anticipate that I will see problems that cannot be dealt with through reallocation in 2004; but if I do, I'll talk to the Secretary and he'll talk within the administration, and we'll do what's right because this is very important to us.

Mr. PLATTS. And that's my focus, that we don't allow a—you know, a paper, a bureaucratic timeframe for submitting a budget request, having to go through the process, being approved; if it is a serious national security issue, that we look at doing whatever we need to do immediately, not when the next budget comes forward.

So I appreciate again your testimonies and your efforts respectively in your offices.

Mr. MAHALEY. Can I add something, Mr. Platts?

Mr. PLATTS. Yes.

Mr. MAHALEY. One thing I notice a lot of concern about, the timing that people should appreciate—and we'll probably get into this in more detail this afternoon—that when you issue a new threat policy, it's essentially a requirements driver. It is analogous in a

very rough way to the Pentagon saying, we are going to plan to fight 2.4 wars or something, and then the Navy and the Air Force resource to meet that requirement.

We've raised a new requirement, OK, for our department. We have superb security police officers deployed throughout the complex, OK—probably not enough of them because of the overtime requirements and everything else, but you just don't snap your fingers and hire those people and do it. It takes a year.

And I'm not talking about the security clearances to get these people on board, train them. We have a minimum 320-hour basic training for our security police officers before they get the site-specific training, and that's just at the basic level. When you get up to your, what we would call the SRT, or SWAT-qualified officers, these are super professionals and it takes time to build officers for that force.

The other point I want to make is that no responsible manager out there should just throw troops at this, OK? They're going to have to take a look and say, I have SNM in that facility. Does it really need to be there? Do I need all of these points of access and egress in this facility? How is this facility designed? Is this facility old?

Are we going to replace it in 2 or 3 years? Build that into the design. There are so many factors. That's a responsible period to bring this in.

Mr. PLATTS. And certainly all valid points. But the fact is that we are approaching 2 years since September 11 now, and now we're just saying, all right, now we have a new design basis threat.

Mr. BROOKS. But please, sir, don't believe we've been sitting around since September 11. I think both of us tried to make clear we——

Mr. PLATTS. I don't believe you are. But we still are almost 2 years since September 11, and that's my point; every day that passes, there's a terrorist individual or group out there that's looking for weaknesses.

And I certainly commend your efforts. I know you take them seriously, your responsibilities and——

Mr. MAHALEY. Mr. Platts, we just finalized an effort. We did issue interim guidance throughout this period. Our people out in the field have been anticipating this.

Mr. PLATTS. I know my time is well expired, so thank you, Mr. Chairman.

Mr. TURNER. Thank you, Mr. Platts.

We will go into a second round of questions.

Mr. Chairman.

Mr. SHAYS. Thank you.

Right now the law requires surveys or the regulations.

Mr. MAHALEY. Regulation. Policy.

Mr. SHAYS. I'm hearing you, Ambassador Brooks, say you want surveillance.

Mr. BROOKS. Correct.

Mr. SHAYS. That we're doing surveillance without the policy saying we are; that's kind of what I'm hearing. So I am a little confused by that.

Mr. Mahaley, maybe you can tell me how that happens and whether it should.

Mr. BROOKS. That's not a fair question to ask him, sir, because he's prohibited by law from telling me what to do. I did it.

Mr. SHAYS. Why don't we have him tell me that?

Mr. BROOKS. I'm sorry, sir.

Mr. SHAYS. Yes, you have a good nature. You want to protect everyone.

Mr. MAHALEY. Essentially what has happened here is, some people think they have a good idea in the NNSA. They have gotten ahead of their headlights, OK? Our policies written in DOE safeguard and security orders call for surveys.

A survey is essentially a very comprehensive checkoff list done by the Federal manager, OK? Surveillance is not this once a year checkoff list; it's a continual monitoring process, if that's fair to say, that's just not contemplated by our policy right now. I don't have any problems with it in theory, but we don't have detailed guidelines for our field offices to use right now. And that's what Linton is talking about in terms of us having developed the policy.

Mr. SHAYS. Right. But intuitively it seems to me it makes sense that you would do that.

But, Ambassador Brooks, you wanted to say——

Mr. BROOKS. I simply wanted to make it clear that if you disagree with what I'm doing, it's not Joe Mahaley's because—no, I think what we have here, we've been trying very hard to move the NNSA in the direction we think it needs to go, and we have occasionally pushed a little bit ahead of the paperwork.

And I'm trying to fix that and get—for example, I made it clear to the site managers what they were responsible for last fall. But we didn't get this formal manual out clarifying that until last month. So we're trying—we're—we are trying to push to improve things as fast as we can while still documenting them accurately.

Mr. SHAYS. OK. The bottom line is, you think it is a good idea. You started to act on it. Mr. Mahaley, you would describe it as getting in front of the headlights. I don't know if I would describe it that way. But, you know, I'll think about it.

I don't quite understand force-on-force exercises. I was looking at a picture in the GAO report of the helicopter. I'm assuming this is, you know, bad guys landing over the line. But what I don't understand is how you can do them and how they work. You would want to tell someone that when five helicopters fly into your site, you don't want to knock them out of the sky, because they happen to be your people just testing the concept.

So I'm asking you a question about the value of force-on-force exercise. How does it work and how do you both respond to it?

Mr. MAHALEY. Well, I actually believe that's a picture of one of our security helicopters at the Savannah River site, deploying a special response team. So they're on our side.

Mr. SHAYS. OK. I have a much greater imagination. I saw them with masks on. But at any rate, let's just say that helicopters are flying in. I don't understand how an exercise works. If you tell people you're going to do it, they're prepared for it.

Mr. MAHALEY. Within programs, they are prepared for it.

Mr. SHAYS. You just tell them a second before, or 5 minutes before?

Mr. MAHALEY. No, sir. You set it up. You have to set up safety briefings.

Mr. SHAYS. Do you tell ground sites?

Mr. MAHALEY. Yes, sir. And within—and there's parameters of when they can attack, what their target is. These are operational sites, and when you do force-on-force, they have to be carefully planned and executed and evaluated.

Mr. SHAYS. OK. So what I'm gathering is, a force-on-force exercise doesn't indicate whether or not you can defend them. They are just really a practice that enables them to go through the process. In other words, you're warning them—let me say it this way.

It would be wrong—would it be wrong for me to interpret that a force-on-force exercise will determine the capability to protect the site? Or are they really nothing more than an exercise?

Mr. MAHALEY. No, I think the—your former summary is probably more correct. And let me explain the process.

Mr. SHAYS. I'm forgetting which was my former summary.

Mr. MAHALEY. That they do have a bearing in determining whether or not the site is satisfactorily protected. They're part of a process that we go through.

Let's look at this this way. We issued a design basis threat. You really can't get down to brass tacks until you apply that design basis threat to a given site, all right? Once you apply that design basis threat, this requirement that the Secretary has set for the site, they then have to analyze how they're going to implement that; and this involves vulnerability assessments of the site, and the goal is going to be to develop a site safeguard and security plan.

In the course of vulnerability assessments and all the models and simulation and the other tools we use, there are going to be hard points that surface. In other words, in some situations, your security forces are going to prevail. It's going to be clear there's not going to be any question.

The areas you want to test on force-on-force are those areas where it's close. And you want to see how your actual forces perform and see if your assumptions about the reaction times and their capabilities are borne out in actual testing.

Now, I would never want to suggest, and I think anybody who's ever seen one or planned one or participated in one would never suggest, that there aren't artificialities, that, you know, they don't necessarily represent what's going to happen, but it's a very effective tool that we use to basically look at the finer points of that site safeguard and security plan.

Mr. SHAYS. I have a red light here. I realize it is a finer tool. I mean, I realize it's a tool to be used. I guess I'm just trying to determine how much we should, on the outside, assess, or you on the inside should assess, your capability to defend. If, in fact, you had to warn people, prepare them, there's not an element of surprise.

Do you ever do the following? Do you ever, all of us, announce that in the next month there will be an attempt to breach the facility and that you will be given a 5-minute warning and go from there and do that?

Mr. MAHALEY. No.

Mr. SHAYS. OK.

Mr. MAHALEY. That's a good way to get people killed, Mr. Chairman. I mean, these are guards who are authorized to use deadly force and armed very well, very well trained. And that's just my personal opinion; I don't think that's the right way to go, not at a nuclear weapons facility.

Mr. SHAYS. I don't want to get people killed.

Mr. MAHALEY. Right, sir.

Mr. SHAYS. However, I don't want to then say that when you have an attempt, when everybody has been briefed thoroughly about it, that it is going to describe to us how easily or well we'll be able to defend a facility, because it does have clear limits.

Mr. MAHALEY. Well, it answers questions, sir. And I think you have to kind of take a whole series of these force-on-force exercises in toto——

Mr. SHAYS. What I am confused about, I am confused why you would be disagreeing with me. Not because I am up here and you're there. It would seem to me the answer would be, yes, sir, it has its limits.

I mean, tell me if you disagree with this: It is a wonderful practice. You're going to see where you have weaknesses, but it isn't going to be able to give us an assessment that we can protect the facility in the way that we might think we can. It's not going to provide all the answers, I guess.

Mr. MAHALEY. That's absolutely correct, sir, absolutely correct.

Mr. SHAYS. But it is an exercise that is helpful.

Mr. MAHALEY. I believe so.

Mr. SHAYS. OK. Thank you.

Mr. TURNER. Mr. Tierney.

Mr. TIERNEY. I have no questions of the witness at this time.

Mr. TURNER. Mr. Ruppersberger.

Mr. RUPPERSBERGER. Yeah, getting back on the oversights, the contractors and, you know, the—there is a problem sometimes with inconsistency.

One of my concerns, you have different levels, level 1, level 2; and could you describe that, please, as far as the type of facility? And yet, any nuclear components getting in the hands of terrorists, wherever they may be, will make a difference. And is there a procedure in place to identify all—a consistent security procedure for both of your levels of plants or operations or sites?

Mr. MAHALEY. I don't want to get into specifics. I'd like to hold that for the closed session this afternoon.

Mr. RUPPERSBERGER. OK. That's fine. Let's get on another issue then.

In order to be able—in management, it starts at the top, but I think good managers listen to the front line. Has there been an assessment from people who are working on the front line that might not have the access to upper-level management, a plan to make a survey, ask questions on what they feel needs to be done as it relates to security?

Mr. MAHALEY. It's kind of funny you ask that, sir. My predecessor, General Gene Habiger, who was the security czar in the last administration, tried to do a survey, and we ran afoul of the Paper-

work Reduction Act and the need to get—you know, we have this funny relationship where we're a Federal agency with 14,000 Feds and 130,000 contractors and we were not able to do that security survey.

But we do get feedback. I get feedback. I just went out to Albuquerque for a national competition. I met with all the site safeguard and security directors. I met with probably about 200 officers. I met the Feds and the contractors, and we encourage that sort of feedback. And by the way, it was a classified session with the site safeguard and security managers and contractors, and we discussed the design basis threat implementation.

Mr. RUPPERSBERGER. Have there been many instances of whistle-blower cases where frontline individuals were trying to get information out?

Mr. MAHALEY. I'm sure there are, and the Department has investigated them.

Mr. RUPPERSBERGER. In my opinion, the front line needs to be heard, to be analyzed to make sure that we are dealing with this type of security. And it is so important that we—part of the analysis of your security must be dealing with that front line.

Mr. BROOKS. I'm concerned with that. We also try in informal ways to sample.

For example, I had some people out looking at an investigation, but just as they were walking, they would talk to protective force officers, get their ideas. I meet with the working level of my site office when I travel; we try and get that feedback.

With respect to whistle-blowers, I want to be very careful here. I don't want to suggest that I am discouraging anybody from communicating with the Congress or the Office of Special Counsel, or within the limits of security, the press.

I am bothered whenever I see somebody who is apparently sincere in wanting to fix things and believes he or she has to go outside the system to do it. There is a cultural—I mentioned earlier that there are cultural issues.

There's a cultural problem at some of my facilities. It's not retaliation. It's not even disinterest in the subject. It's oh, I'm busy, don't bother me. I don't know what it is, but I'm trying to work on that.

Mr. RUPPERSBERGER. And I'm not trying to go there with respect to the issues of whistle-blowers. I'm looking at the total assessment. When you have partnerships between business and government and you're dealing with national security, there needs to be an assessment of what's happening. And a lot of times we, up top at the highest level, don't get the information. And sometimes the front line gets it.

I just want to make sure, or that's why I'm asking the questions, the consistency of your security programs, consistency between level 1 and level 2.

Let me get into another level. We talked about physical security. How about the computer networks, I mean, which is an important part also? Where are we with respect to that?

Mr. BROOKS. I think I'd refer you to Mr. Podonsky's prepared statement, and what he will tell you is, we're in good shape on the classified networks; that we are—we don't have any—I mean, cyber

security is an infinite ladder; you can always make it better. But we don't have significant problems on the classified networks.

On the unclassified networks, there are some problems that have been identified that we're trying to work on. And those problems are whether or not we are strong enough not just to defeat the external hacker sitting in a basement somewhere, but for example, in one of our facilities where we have—because these are scientific laboratories, we have foreign nationals, whether we are segmenting the unclassified network as thoroughly as we might.

We've had another problem recently in which someone was obtaining salary data on an unclassified network. You're not supposed to be able to do that.

So I don't think that it is serious in terms of national security because, by definition, unclassified information is unclassified. In terms of sound management, we've got a ways to go on the unclassified side in our cyber security, at least at my sites.

Mr. RUPPERSBERGER. OK.

Mr. TURNER. Gentlemen, I want to thank you for your testimony here today and certainly for your efforts. As you're aware and as has been said earlier in the hearing, we're having a closed session this afternoon so that we can have a greater discussion of issues surrounding this that are classified; and in recognition that we have the closed session, I wonder if either of you have anything else you wanted to add to the record in this public session.

Mr. BROOKS. No.

Mr. MAHALEY. No, thank you.

Mr. TURNER. OK. Thank you very much.

Mr. SHAYS. If I could, Mr. Chairman.

Mr. TURNER. Yes.

Mr. SHAYS. What we'd like you to think about, you have the prerogative to testify separately when we go into the closed session. We might be able to cover the issues if we do it in a larger panel. That'll be your decision.

You can talk to us later, but if you let my staff know whether you would want to go separately and have to wait, or whether we all go at once and try to cover it that way, OK?

Thank you. Thank you all very much.

Mr. MAHALEY. Thank you sir.

Mr. SHAYS. Thank you, Mr. Chairman.

Mr. TURNER. Turning to our third panel, which will include Danielle Brian, executive director, Project on Government Oversight, and Ronald Timm, president of RETA Security, if you would both stand——

[Witnesses sworn.]

Mr. TURNER. Please let the record note that the witnesses responded in the affirmative.

Ms. Brian.

STATEMENTS OF DANIELLE BRIAN, EXECUTIVE DIRECTOR, PROJECT ON GOVERNMENT OVERSIGHT; AND RONALD E. TIMM, PRESIDENT, RETA SECURITY

Ms. BRIAN. Mr. Chairman, I commend you for holding these important hearings.

The Project on Government Oversight is an investigative organization that works with inside sources to improve public policy. We are a politically independent nonprofit watchdog that strives to promote a government that's accountable to the citizenry.

In early 2001, POGO began its investigation into nuclear security at the Department of Energy after more than a dozen high-level departmental security experts came forward with their concerns. We interviewed, after that, current and former DOE security officials, Special Forces personnel who test security at nuclear facilities and DOE contractors, such as Mr. Timm, who coauthored the report. We now have people contacting us from all over the complex and headquarters.

Just prior to September 11, 2001, POGO issued our report; and I ask that it be included in the record, but maybe just the text, because the attachments make it really fat.

[The information referred to follows:]

POGO

Project On Government Oversight
Watchdog since 1981

U.S. Nuclear Weapons Complex: Security at Risk

666 Eleventh Street, NW
Suite 500
Washington, DC 20001-4542
202/ 347-1122
202/ 347-1116 Fax
pogo@pogo.org
www.pogo.org

October 2001

R E P O R T

POGO MISSION STATEMENT

The Project On Government Oversight (POGO) investigates, exposes, and seeks to remedy systemic abuses of power, mismanagement, and subservience by the federal government to powerful special interests. Founded in 1981, POGO is a politically-independent, nonprofit watchdog that strives to promote a government that is accountable to the citizenry.

Danielle Brian
Executive Director
Project On Government Oversight
666 Eleventh Street, NW, Suite 500
Washington, DC 20001-4542
(202) 347-1122 Fax: (202) 347-1116
www.pogo.org email: pogo@pogo.org

Table of Contents

Foreword i

Executive Summary 1

Introduction 4

Examples of Recent Vulnerabilities 5

Background on DOE Nuclear Weapons Complex 7

DOE Map of Plutonium Inventories 8

The Design Basis Threat 9

Three Case Studies 11
- Rocky Flats 11
- Los Alamos Technical Area-18 15
- Transportation Security Division 17

Major Threats to the Complex 19
- Weapons of Mass Destruction 19
- Truck Bombs 20
- The Creation of an Improvised Nuclear Device 21
- Theft of Nuclear Secrets 21

Misleading Test Results – And they Still Lose 50% of the Time 23
- Dumbed-down Security Tests 23
- Overstatement of Protective Force Combat Effectiveness 26

Security Oversight – A Weak Record 27
- Up the Security Chain of Command 27
- National Nuclear Security Administration
  - Different Name, Same Problem 32
- Lack of Congressional Oversight 33

Rewards and Punishment Turned On Its Head 34
- Promotions for Security Failures 34
- Whistleblowers: Shooting the Messenger 35

Budget 38

PROBLEMS/SOLUTIONS 39

Appendices Table 43

Acronym Glossary 47

Foreword

This report presents the results of an eight-month investigation initiated when more than a dozen whistleblowers contacted POGO with unclassified evidence that the U.S. Department of Energy's nuclear bomb complex is vulnerable to a terrorist attack.

The contents of this report have been reviewed by trained and certified classifiers from inside and outside the government to ensure that this report contains no classified information.

Report Contributors

POGO Staff
Danielle Brian, Executive Director
Lynn Eisenman, Research Assistant
Keith Rutter, Director of Operations

Peter Stockton, is a paid consultant with POGO. He was Special Assistant to DOE Secretary Bill Richardson from 1999-2001. Mr. Stockton was the Chief investigator for Chairman John Dingell (D-MI) of the House Energy and Commerce Committee from 1972-1995, including during the Committee's investigations of DOE security failures.

Unpaid Contributors: Ron Timm, RETA Security President, Security Analyst hired by DOE to analyze security at DOE weapons facilities. The additional contributors to this report have requested anonymity for fear of retaliation for exposing security failures. They include DOE security analysts, current and former Special Forces who portray mock-terrorists in force-on-force drills, DOE contractors, and officials at various levels of DOE Headquarters and facilities.

Executive Summary

The Department of Energy (DOE) analyzes and tests the security of nuclear weapons facilities by conducting simulations and mock force-on-force exercises, often using U.S. military forces as adversaries. The government requires that nuclear facilities be able to defend against theft of nuclear materials or radiological sabotage by a few terrorists using surprise and readily available weapons and explosives, as well as against the theft of nuclear secrets.

According to experts who have conducted these tests in the past, the government fails to protect against these attacks more than 50% of the time – although the exact figure is classified. For example, in a test at the Rocky Flats nuclear production facility, Navy SEALs successfully "stole" enough material to make multiple nuclear weapons. In a test at a Los Alamos facility, the "terrorists" had enough time to construct an Improvised Nuclear Device. In addition, the theft of nuclear secrets remains as possible today as it was several years ago before the controversy over the downloading of classified information at Los Alamos.

DOE employees and others who have raised security concerns have largely been ignored and subjected to retaliation over many years. This report details several case studies of whistleblowers being fired, being forced to resign, losing contracts or losing security responsibilities because they were unwilling to quietly accept the inadequate security measures at DOE nuclear facilities. In one example, in a desperate attempt to raise public awareness last year about these problems, a DOE employee faxed two unclassified Inspector General reports to *USA Today* and the *Washington Post*, which highlighted the Department's failure to take corrective measures. His security clearance was suspended and he is no longer working on security issues.

DOE's disregard for proven threats to nuclear security and its institutional bull-headedness has thwarted the efforts of reformers, time and time again. According to a review by Senator Warren Rudman, "scores of critical reports from the General Accounting Office (GAO), the intelligence community, independent commissions, private management consultants, its Inspector General, and its own security experts...the Department's ingrained behavior and values have caused it to continue to falter and fail."

Ten major sites have weapons-grade plutonium (PU) and highly-enriched uranium (HEU) in sufficient quantities to make a nuclear device even though most of them have not had a national defense mission since the end of the Cold War. Several of these sites are located near major metropolitan areas including the Bay area of Northern California; Denver, Colorado; Albuquerque, New Mexico; and Knoxville, Tennessee (see chart on page 7). In addition, the DOE Transportation Safety Division regularly moves weapons-grade nuclear materials and nuclear weapons between facilities across the country. Because many tons of weapons-grade nuclear materials are at these facilities, a nuclear detonation at one of them would dwarf the impacts of Chernobyl, potentially kill or injure millions of Americans, and destroy the environment of a significant portion of the United States.

The Project On Government Oversight (POGO) has conducted a series of interviews and consultations with nuclear security and terrorism experts to identify the following major problems with nuclear facility security and their solutions:

PROBLEM: Nuclear Materials Are Spread Across the Country. Weapons-quantity special nuclear materials are stored at 10 fixed sites even though most have virtually no national security mission. DOE cannot currently adequately protect this material, and security at each site unnecessarily increases redundancies and costs. Not only do the unnecessary sites cost the taxpayers billions annually, but they also present a significant health and safety risk to nearby communities.

➤**SOLUTION: Close Unneeded Facilities.** The Base Realignment and Closure Commission should be empowered to recommend closing the unneeded and redundant DOE sites, as well as those sites that have no national defense mission. The Bush Administration is considering this step.

➤**SOLUTION: Consolidate Nuclear Materials.** Two of the most secure facilities in the world would provide enough storage for the entire DOE weapons complex – a secure underground weapons storage facility at Kirtland Air Force Base in New Mexico and the Device Assembly Facility at the Nevada Test Site.

➤**SOLUTION: Immobilize Excess Nuclear Materials.** There is a facility at Savannah River which could be used to meld excess nuclear materials with a radioactive barrier in glass. Once the materials have been immobilized or "vitrified", they would no longer be useful to terrorists.

PROBLEM: Bureaucracy Makes Security Tests Easier Rather than Fixing Problems. The DOE bureaucracy portrays facilities as being secure and impervious to terrorists and spies when, in fact, they are not.

➤**SOLUTION: Improve Effectiveness of Protective Forces.** Until disparate sites are consolidated, DOE should increase the size of its protective force and improve weaponry, tactics, and command, control, and communication to defend against both theft and radiological sabotage. Federalizing protective forces or exploring use of the military are two options.

PROBLEM: Independence in Nuclear Security is Lacking. The recently Congressionally-created National Nuclear Security Administration (NNSA) exacerbates the problem by elevating the same people who have managed this debacle over the last three decades.

➤**SOLUTION: Take Security Management Out of DOE.** POGO suggests exploring the option of setting up an independent agency to provide security from outside DOE entirely, and leave the many other duties of managing the nuclear weapons complex to the NNSA.

➤**SOLUTION: Move the Independent Oversight Office Out of DOE.** Make oversight of nuclear security independent from those charged with implementing security by making the DOE Office of Independent Oversight an Independent Nuclear Facilities Security Board that is independent of DOE. A model would be the Defense Nuclear Facilities Safety Board. This board would report directly to the Congress and be empowered to assess security in the nuclear complex.

PROBLEM: Computers Containing Nuclear Secrets Remain Vulnerable. It is virtually as easy today for a trusted "insider" to put weapons design information on a tape or disk and walk out the door as it was during the controversy at Los Alamos. All of our known spies have been insiders with the highest security clearances.

➤**SOLUTION: Convert to Media-less Computing.** The only way to stop an "insider" is to stop any media (disks, tapes, laptops, etc.) from coming in or out of priority classified areas. Computers would be locked in vaults and access to any media would require a "two-man rule" where two people would have to sign-off on any copies.

PROBLEM: DOE Security Forces Cut by 40%. According to a high-level DOE official, "Since 1992, the number of Protective Forces at DOE sites nationwide has decreased by almost 40% (from 5,640 to the current number of approximately 3,500) while the inventory of nuclear material has increased by 30%." The increase has resulted from the dismantling of nuclear weapons and the receipt of nuclear materials from the Former Soviet Union. During the same period the threat of terrorism has increased.

➤**SOLUTION: Consider Security Budgetary Needs Independently.** Decouple nuclear security funding from scientific research and the nuclear weapons program. Security funding currently competes with scientific research funding from within the National Nuclear Security Administration nuclear weapons budget. Security is always fighting for the scraps after the more politically appealing and bureaucratically popular scientific research and weapons projects are funded.

Introduction

The chances that chemical, biological or nuclear terrorism will occur on U.S. soil over the next ten years "is 100%," according to Richard Clark, U.S. National Security Council National Coordinator for Infrastructure Protection and Counterterrorism for the Clinton and Bush White Houses.

Over a dozen whistleblowers have contacted the Project On Government Oversight (POGO) with unclassified evidence that the U.S. nuclear bomb complex, containing tons of weapons-grade uranium and plutonium, is vulnerable to a terrorist attack. The particular vulnerabilities discussed in this report have been addressed by the Department of Energy (DOE), thereby making them no longer classified. However, new as well as recurring vulnerabilities continue to plague DOE's nuclear security program. This evidence confirms the findings of multiple Presidential and DOE Commissions. Such an attack would endanger the health and safety of the communities near each site to levels in excess of the accidental release at Chernobyl.

The DOE tests the security of these sites by conducting simulated and mock force-on-force exercises often using military forces as the adversary. The government requires that these sites be able to defend against theft of nuclear materials or radiological sabotage by a few terrorists using surprise and readily available weapons and explosives, as well as against the theft of nuclear secrets. According to experts who have conducted these tests in the past, the government fails to protect against these attacks more than 50% of the time – although the exact figure is classified. In addition, the theft of nuclear secrets remains as possible today as it was two years ago when controversy surrounded Los Alamos National Laboratory over the possible leaking of classified information.

As a result of that controversy, in June of 1999, the Chair of the President's Foreign Intelligence Advisory Board, former Senator Warren Rudman (R-NH) was asked to review security at the DOE nuclear weapons laboratories. Their report, "Science at its Best, Security at its Worst" was startlingly blunt in their criticism: ". . . the brilliant scientific breakthroughs at the nuclear weapons laboratories came with a very troubling record of security administration. . . . This report finds that DOE's performance, ***throughout its history***, should have been regarded as intolerable."[1] (Emphasis added)

More importantly, the Rudman report points out the longevity of these problems and the institutional hubris that continues to perpetuate them: "Second only to [DOE's] world-class intellectual feats has been its ability to fend off systemic change." Former Energy Secretary Richardson did much to promote institutional reform in the area of nuclear security, including bringing people in from outside the DOE bureaucracy to oversee nuclear security – specifically General Eugene Habiger and General John Gordon. However, Rudman points out that "the

[1] http://fas.org/sgp/library/pfiab/ – Downloaded September 13, 2001.

Department's bureaucracy is quite capable of undoing Secretary Richardson's reforms, and may well be inclined to do so."

DOE's disregard for proven threats to nuclear security and its institutional bull-headedness has thwarted the efforts of reformers, time and time again. Regardless of "scores of critical reports from the General Accounting Office (GAO), the intelligence community, independent commissions, private management consultants, its Inspector General, and its own security experts . . .the Department's ingrained behavior and values have caused it to continue to falter and fail." The report goes on to emphasize this point:

> "***More than 25 years worth of reports***, studies and formal inquiries – by executive branch agencies, Congress, independent panels, and even DOE itself – have identified a multitude of chronic security and counterintelligence problems at all of the weapons labs. These reviews produced ***scores of stern, almost pleading, entreaties for change***. Critical security flaws – in management and planning, personnel assurance, some physical security areas, control of nuclear materials, protection of documents and computerized information, and counterintelligence – have been ***cited for immediate attention and resolution . . . over and over and over . . . ad nauseam***." (Emphasis added)

Finally, the Rudman report states, "The panel has found that DOE and the weapons laboratories have a deeply rooted culture of low regard for and at times, hostility to security issues . . . The Department of Energy is a dysfunctional bureaucracy that has proven it is incapable of reforming itself. . ."[2]

More recently, in June of 2001, then-Chair Fred Thompson (R-TN) of the Senate Governmental Affairs Committee, highlighted the Department of Energy – and particularly their poor handling of security – in its report "Government at the Brink: An Agency by Agency Examination of Federal Government Management Problems Facing the Bush Administration."[3]

Examples of Recent Vulnerabilities

In October 2000, during a force-on-force drill at Los Alamos, New Mexico, the mock terrorists gained control of sensitive nuclear materials which, if detonated, would have endangered significant parts of New Mexico, Colorado and downwind areas. (Appendix A[4])

---

[2] Ibid.

[3] http://www.senate.gov/~gov_affairs/vol2.pdf – Downloaded on September 17, 2001.

[4] At the time this memo was written, this particular vulnerability had not yet been resolved, thus the identity of the facility was classified. Since that time, this particular vulnerability has been addressed to the satisfaction of General Gordon and the Office of Independent Oversight, making this information no longer classified. Details described in the memo, such as the "garden cart incident" and the plans for relocation, have since been attributed to TA-18 at Los Alamos National Lab, by Appendices T, V, & BB.

In an earlier test at the same location, a U.S. Army Special Forces team was able to "steal" enough weapons-grade uranium for numerous nuclear weapons and was able to carry the extremely heavy material with the use of a Home Depot garden cart – throwing the protective forces into disarray. The DOE argued that this test attack was unfair. (Appendix A)

In another exercise, Navy SEALs were able to make a hole in a chainlink fence surrounding Rocky Flats near Denver, Colorado, undetected and easily "stole" enough plutonium for several nuclear bombs. They were only discovered as they were successfully leaving the facility.

The Department of Energy Transportation Security Division moves nuclear weapons, as well as weapons-grade uranium and plutonium, from site to site across the nation on public highways. Over the last several years, there have been exercises testing the security of this Division where the DOE security force failed to protect nuclear cargo because they had inadequate weapons and insufficient numbers, as well as poorly conceived tactics. Due to these insufficiencies, the protective forces were defeated in six out of seven exercises in December 1998. (Appendix B)

In 1998, the Fall of 1999, and again in the Spring of 2000, two force-on-force exercises were run to test the Rocky Flats protective force. A "criticality alarm" – warning that a nuclear chain reaction is potentially imminent – was set off creating confusion, allowing the "terrorist" access to special nuclear materials. Such an alarm requires everyone to immediately leave the building. Hoping to "kill" the "adversaries" the protective force "indiscriminately shot" employees, controllers and each other as they were exiting the building in response to the alarm.[5] The protective force count these tests as successes because they kill all the adversaries – although they also killed all the employees and several of the protective forces as well. (Appendix C)

In addition to physical security, there also remain cyber security weaknesses. The major threat to the compromise of critical nuclear weapons information is the "trusted insider" – personnel with the highest security clearances. Voluminous amounts of information can be accessed quickly and easily. For example, a device the size of a Gameboy can download the equivalent of 1100 floppy discs off a computer in 3 minutes and 14 seconds. Another device called a memory stick, smaller than a stick of gum, can download the equivalent of 44 floppy disks in a couple of minutes. Incredibly, DOE has done virtually nothing effective to protect against the "insider" working on classified computers despite the many Congressional hearings and increased media scrutiny generated by the Los Alamos controversy.[6] (Appendix D)

---

[5] The protective force and mock terrorists are outfitted with Multiple Integrated Laser Engagement System (MILES) weapons laser-simulation equipment.

[6] http://fas.org/sgp/library/pfiab/ – Downloaded September 13, 2001.

Background on DOE Nuclear Weapons Complex

The U.S. nuclear weapons complex managed by DOE is spread across the country. Ten major sites have weapons-grade plutonium (PU) and highly-enriched uranium (HEU) in sufficient quantities for a nuclear device. Several of these sites are located near major metropolitan areas with large populations. (See chart below.) In addition, the DOE's Transportation Safety Division (TSD) moves weapons-grade Special Nuclear Materials (SNM) across the country on interstate highways. Although the total inventory of PU and HEU is classified, according to "DOE Facts" sheets, there are 994 metric tons of HEU[7] and 33.5 metric tons of PU (Appendix F), excluding the PU inventories at Pantex which remain classified. According to the Nuclear Control Institute, it takes less than 50 pounds of HEU or PU to craft a crude nuclear device.[8] In addition, there are significant quantities of completed nuclear weapons, and huge quantities of weapons in various stages of assembly and dismantlement – including those that have been stored for decades as a "war reserve" – that would be attractive to terrorists. The following DOE map shows the location of weapons-grade plutonium inventories. The eight sites identified with plutonium on the map, as well as the Oak Ridge National Laboratory in Tennessee and Sandia National Laboratory in New Mexico, also hold highly enriched uranium inventories.

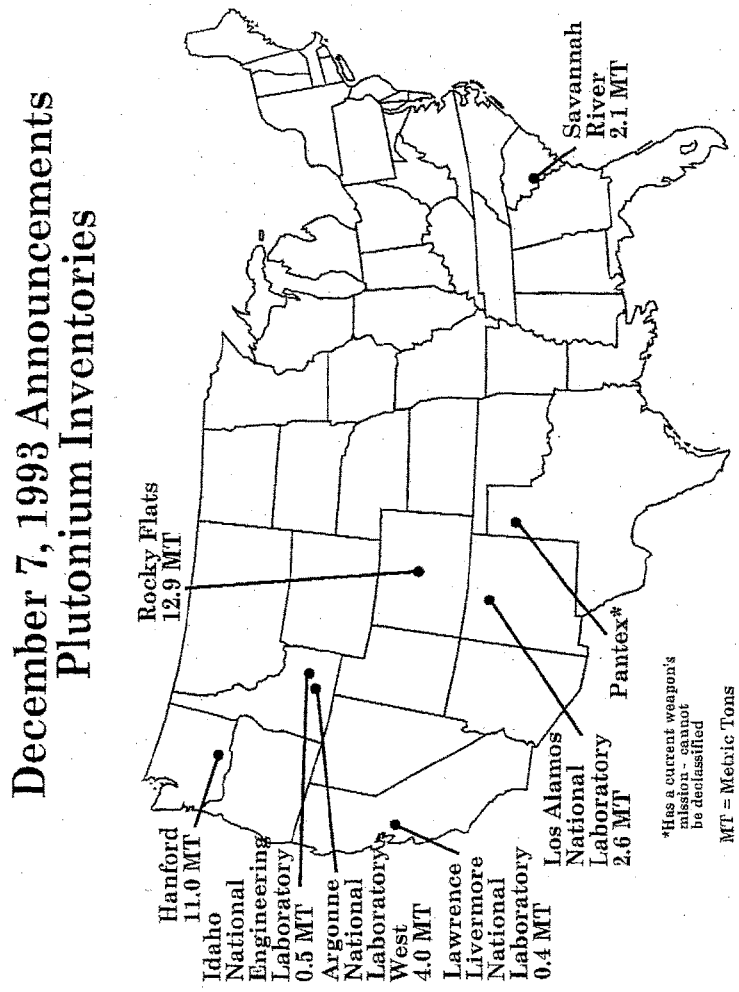
Metropolitan Areas Within 100 miles of Nuclear Weapons Facilities[9]

Site Name	Metropolitan Area	Population
Lawrence Livermore	San Francisco-Oakland-San Jose, CA	7,039,362
Rocky Flats	Denver, CO	2,581,506
Sandia	Albuquerque, NM	712,738
Oak Ridge	Knoxville, TN	687,249
Savannah River	Augusta-Aiken, GA-SC	477,441
Pantex	Amarillo, TX	217,858
Hanford	Richland-Kennewick-Pasco, WA	191,822
Los Alamos	Santa Fe, NM	147,635
Argonne & Idaho National	Pocatello, ID	75,565

[7] http://www.osti.gov/html/osti/opennet/document/press/pc13.html - Downloaded September 25, 2001.

[8] http://www.nci.org/new/nci-pro.htm - Download September 26, 2001.

[9] Figures compiled from U.S. Census, Metropolitan Areas Ranked by Population 2000. http://www.census.gov/population/cen2000/phc-+3/tabo3.pdf – Downloaded as of September 17, 2001


December 7, 1993 Announcements
Plutonium Inventories
Hanford
11.0 MT
Idaho
National
Engineering
Laboratory
0.5 MT
Argonne
National
Laboratory-
West
4.0 MT
Lawrence
Livermore
National
Laboratory
0.4 MT
Rocky Flats
12.9 MT
Los Alamos
National
Laboratory
2.6 MT
Savannah
River
2.1 MT
Pantex*
*Has a current weapon's
mission - cannot
be declassified
MT = Metric Tons
Total = 33.5 MT

An issue that exacerbates security problems is the age of these sites and the decay of the infrastructure. Oak Ridge, Savannah River, Hanford and Los Alamos, for example, were all built for the Manhattan Project in the 1940's. The isolated location of these sites made sense at the time for safety and security reasons. Now, population growth and more mobility have made a number of the sites extremely difficult to protect. For example, Technical Area-18 (TA-18) at Los Alamos, New Mexico, with tons of PU and HEU was built in a canyon to absorb the radiation from the reactors. TA-18 also houses several moveable burst nuclear reactors, which are small machines, from the size of a bowling ball to as large as 4 feet by 4 feet by 5 feet tall, containing PU and HEU fuel. The site is extremely vulnerable because terrorists could easily occupy the unprotected high ground around the canyon. A public highway passes within a few feet of the fence line and the facilities that house the PU and HEU. The infrastructure around many of these sites is in decay including storage facilities, fences, and alarm systems.

The Design Basis Threat

There is a classified "Design Basis Threat" (DBT) that describes the level of threat the contractor is required to defend against – the number of outside attackers and inside conspirators, and the kinds of weapons and explosives that would be available to terrorists. (Appendix G) The process that determines this threat was described by Edward McCallum, the former Director of the Office of Safeguards and Security in a letter to the Director of the Office of Security Affairs: "The FBI, CIA, DOE, and the military services as well as the Nuclear Command and Control Staff have developed the existing Design Basis Threat over a number of years. It has been extensively reviewed and supported by studies issued by the DIA [Defense Intelligence Agency]. Sandia, as well as the other labs, have been asked to comment and participate in the development process." (Appendix H)

Each site is then required to develop a Site Safeguards and Security Plan (SSSP) annually, which describes in detail how they would counter the most likely and most disastrous attack scenarios based on the DBT. The plan is developed by the contractors, and then analyzed and approved by the DOE field office and various Headquarter's program offices to confirm that the site is at low risk.

Despite the fact that the DBT goes through this studied, interagency process, the bureaucracy often complains that it is too high a standard to meet – "defending against that terrorist that is about thirteen feet in height" (Appendix E) or super-terrorists. But in fact, the DBT does not require DOE to defend against exotic weapons, but weapons that are readily available on the open market from private arms dealers. According to DOE's Independent Oversight Office, the opposite is true and in fact the capabilities of terrorists are underestimated in the planned scenarios:

> **"Capabilities of Available Adversary Weapons Are Not Being Accurately Represented.** In the last year this office has catalogued a long list of readily available adversary weapons and tools that are not being used appropriately by the adversaries depicted in current SSSP/VAs. Among these are tactical smoke, irritant gases, anti-personnel and anti-vehicle explosive devices ("stay-behinds"), grenades, armor-piercing small arms ammunition, and communications disruption devices, to name but the most obvious. It has become "customary" in DOE to limit the use of such weapons and tools, creating the potential for artificially high calculations of protective force effectiveness." [This is inconsistent with tactics currently being taught in the Afghanistan training camps and used by terrorist groups in Columbia, the Philippines, Sri Lanka, Chechnya, the Balkans, and the Middle East.] (Appendix I)

The Design Basis Threat specifies that sites are only expected to protect against:

> "A small group (including an insider)" [the actual number is classified]
>
> **"Characteristics:**
>
> - Capable of lethal and violent action; willing to kill and be killed.
> - Capable of conducting coordinated paramilitary operations.
> - Possess a wide range of military equipment, weapons and ordnance.
> - Access to funds, communications, transportation and safehouses." (Appendix G)

This Design Basis Threat intends to protect nuclear weapons facilities from:

- Theft of nuclear material;
- Radiation sabotage – blowing up nuclear material and dispersing radiation into the surrounding areas (this could be achieved by an insider, an outside terrorist getting inside or more likely, with a truck bomb); and
- Exploding PU or HEU in such a way that it causes a nuclear chain reaction, through the creation of an Improvised Nuclear Device that could result in Hiroshima-like devastation. How such a crude weapon could be created is highly classified, however, experts point out that any self-respecting college physics student already has that knowledge. Explicit instructions on how to build a nuclear weapon are on the internet.

It is difficult to deal with the failures of DOE security because of the level of classification of information regarding the nuclear weapons complex. Of course, some classification is legitimate, but a good deal of information is classified because it is embarrassing.

Three Case Studies

Three case studies provide an insight into how the system has failed: the plant at Rocky Flats, outside of Denver, Colorado; Technical Area-18 (TA-18) at Los Alamos, New Mexico; and the Transportation Security Division, which travels the United States interstate highways. The repetition of problems in these case studies should make it clear that these problems are systemic, constant and recurring.

Rocky Flats

Rocky Flats, outside Denver, Colorado, was a major weapons production facility during the Cold War where the plutonium parts for nuclear weapons were milled and fabricated. Tens of tons of plutonium as well as uranium are stored at Rocky Flats. DOE is currently in the process of shutting down the plant and de-inventorying – sending the PU to Savannah River and the HEU to Oak Ridge. Currently, there are still large quantities of Special Nuclear Materials (SNM) at Rocky Flats that are attractive to terrorists. Wackenhut Security, a private security firm, supplies the protective force. Kaiser-Hill LLC is the prime contractor managing Rocky Flats.

In 1992, members of the Wackenhut security force were upset because they argued federal oversight was too overzealous. This tension between federal overseers and the contractor is highly unusual in the DOE complex. In a July 16, 1992 letter to Terry Vaeth, DOE Manager at Rocky Flats, Timothy P. Cole, President of Wackenhut Services Incorporated stated, after taking over security at the site in July 1990:

> "During our first few months we were racing to prepare for an upcoming DOE OSE Inspection and Evaluation. Further, the plant mission was undergoing intense scrutiny based on safety and environmental concerns. Those priority issues coupled with fundamental security needs put us in a position of vulnerability from a performance measurement standpoint. There weren't enough hours in the day. The Protective Force supervisory ranks and the number of cleared, trained Security Inspectors were inadequate for accomplishment of the security mission . . .
>
> "The purpose is not to make excuses, explain away, or otherwise disclaim our performance deficiencies. We have privately and publicly accepted responsibility for all of our actions and stepped up to problems and emphasized corrective actions rather than arguing the issues. . . .

> "I must tell you very frankly that we have been exposed to 'management terrorism' and 'organizational sedition' for well over a year. . . .
>
> "The DOE management oversight process at RFO [Rocky Flats Office] is, in my opinion, heavily slanted toward the negative to include specific 'targeting' of people in management as well as individual members of the Protective Force." (Appendix J)

As even Cole acknowledged, Wackenhut was having trouble performing some basic security duties. For example according to sources, in a surprise security test at that time, federal security overseers passed through a secured entrance with a pistol in a coffee can – an obvious breach of security.

Wackenhut President Timothy Cole's letter warned Rocky Flats federal security officials, "The distrust, doubt and fear our Security Inspectors have for certain DOE officials is unhealthy and *may lead to serious consequences*." (Emphasis added) The federal Director of Security was removed, and Wackenhut retained their contract. (Appendix J)

In 1995, two Wackenhut security force whistleblowers, Mark Graf and Jeff Peters, wrote to their Congressman, David Skaggs (D-CO), citing their concerns about the poor security at Rocky Flats being performed by Wackenhut. Their whistleblowing lead to a harrowing sequence of retaliations against both Graf and Peters, including their being sent for psychiatric evaluations. After both were put on administrative leave, Peters resigned. Graf was reinstated after winning his whistleblower retaliation lawsuit.[10]

The federal Office of Personnel Management interviewed Wackenhut Services Inc. (WSI) General Manager William R. Gillison during the Jeff Peters whistleblower case. Gillison acknowledged that he, "reported to WSI Corporate that the SNM was at high risk and it was not WSI's responsibility to assume responsibility for such material." (Appendix K)

In 1996, according to sources, DOE Headquarters rejected the Site Safeguards and Security Plan (SSSP) citing serious deficiencies.

In January 1997, the DOE "Report to the President on the Status of Safeguards and Security for 1996" gave Rocky Flats a marginal rating – meaning that nuclear material was not being protected adequately. (Appendix L)

---

[10] http://www.whistleblower.org/www/grafexcerpt.htm – Downloaded on September 17, 2001.

In March 1997, DOE determined that Rocky Flats was in fact not marginal, but "that there were vulnerabilities at the site that were not identified or addressed in the 1997 SSSP and that SNM was at risk under the then existing conditions." (Appendix M)

In April 1997, a subsequent Director of Security for DOE at the Rocky Flats site, Col. David Ridenour, resigned because he believed the health and welfare of the public was not being protected, and that top management would not allow him to perform his duties. He wrote in a letter to the Head of the Operations Office, "In my professional life as a military officer, as a Registered Professional Engineer. . . I never before experienced a major conflict between loyalty to my supervision and duty to my country and to the public. I feel that conflict today." (Appendix N)

The next week in April 1997, Col. Ridenour wrote in a letter to then-Secretary of Energy Federico Pena ". . . I was instructed by my direct supervisor . . . that my mission was to 'not negatively impact the contractor' and that I was to 'facilitate the contractor (a joint venture between Kaiser and CH2M Hill) winning the award fee'." (Appendix N)

In September 1997, again the SSSP was rejected. DOE Headquarters gave Rocky Flats 120 days to implement corrective actions. After 120 days, no action had been taken, and no one was held accountable – neither government employees nor contractors (Appendix M)

In 1997, unauthorized taped phone calls with DOE Headquarters Director of Security Col. Edward McCallum by Wackenhut whistleblower Jeff Peters revealed McCallum's concern that terrorists could gain access to large quantities of plutonium and cause a sizable nuclear detonation. McCallum stated, "I've said in front of the Deputy Secretary and people at that level, I think the citizens, the employees at the plant, and the citizens of Colorado are at extremely high risk for no reason." These concerns were first raised in 1995 – two years earlier – yet they had remained unresolved. (Appendix O)

In January 1998, the Independent Oversight team from DOE Headquarters conducted a force-on-force at Rocky Flats, concluding that security was "adequate by a narrow margin." For the third time, another SSSP was submitted and rejected by Headquarters – the site was not at low risk. (Appendix Q)

In May 1998, Deputy Assistant Secretary Glenn S. Podonsky of the Office of Independent Oversight and Performance Assurance (heretofore the Office of Independent Oversight) wrote that after a comprehensive inspection, ". . . the protection program elements measured during this inspection do not indicate that a fully effective program is yet in place. As evidenced by deficiencies identified in some areas of physical security systems, material control and accountability, computer security, and classified matter protection and control, there remain a number of legacy safeguards and security issues to be resolved." (Appendix P)

Several whistleblowers attended a summer 1998 briefing of all DOE Security Directors at Savannah River Site near Aiken, SC, by a Navy Captain regarding force-on-force drills conducted by the Navy SEALs at Rocky Flats. During the tests, the SEALs successfully entered the site through the perimeter fence, getting into a nearby building, and "stealing" a significant quantity of plutonium, exiting the building, getting out through the fence and escaping without being caught. After this embarrassment, for the next two force-on-force tests, Rocky Flats management "over controlled" and demanded that the SEALs could not go through the same hole from which they came in – they had to take the plutonium and climb a guard tower and rope it over the fence. (Of course, real terrorists could have just thrown it over the fence.) In these two contrived tests, the protective force successfully defended the facility. According to the whistleblowers, the SEAL Captain announced he would never waste the time of the SEALs coming back to a DOE site, because the tests were unrealistic.

In July 1999, then-Energy Secretary Bill Richardson sent a security team to Rocky Flats. Two glaring vulnerabilities were found, strikingly similar to those found in 1995 and again in 1997. Rocky Flats management vehemently denied the team's accusation that plutonium was kept out of the vault without additional protective forces in place, as is required. Several hours later in the meeting, they finally admitted they had plutonium out of the vault in a high-risk situation eight hours a day, five days a week. (Appendix R) The significance of this dangerous practice was highlighted when, according to security team members, only a few weeks earlier an employee had walked out of a key security door setting off the alarm – yet the protective force could never find the employee. Because the PU was inadequately protected, the employee could have taken some of it, walked out and thrown it over the fence – never to be discovered.

Also according to sources, the security team found the vehicle barrier on the wrong fence. A vehicle barrier is a heavy steel cable – strong enough to stop a speeding truck loaded with thousands of pounds of explosives – that should be attached to the inside fence of a two-fence perimeter. The Rocky Flats cable was on the outside fence, which does not have alarms. Therefore a terrorist could, undetected, cut the cable and drive through the outside fence, easily crash through the inside chain link fence in a truck loaded with explosives, park alongside a nearby vault, and detonate a bomb. This vulnerability had been identified in 1996, and had never been fixed. In late 1999, under pressure from Richardson's team, this problem was addressed within hours at minimal cost by placing large boulders around the fence.

In October 1999, the DOE security czar sent DOE and DOD experts to Rocky Flats to resolve the outstanding problems found by Richardson's team. At first, Rocky Flats DOE management refused to allow the team on the site. Once they were permitted inside, the experts still found the same problems Rocky Flats had agreed to fix two years earlier.

When the experts returned in March 2000 to validate the protective force changes, they found a different but alarming trend. Repeatedly during force-on-force drills, the protective forces were "shooting" everyone in sight – mock terrorists, scientists, "controllers wearing orange safety vests, and each other" – in a simulated test. The rules of deadly force were

completely abandoned to pass the tests and prove "low risk," the same problem noted in 1998 and again in 1999. This pattern is described in more detail on page 25. (Appendix C; Appendix M)

Los Alamos Technical Area-18

Technical Area-18 (TA-18), run by the University of California, is one of a number of technical areas at Los Alamos. It houses several nuclear burst reactors and tons of weapons-grade HEU and PU. The facility was built on the floor of a canyon in the 1940's so that the walls of the canyon would absorb the radiation from the reactors. However, today the lack of control of the high ground around the canyon makes the site extremely difficult to defend.

Special Nuclear Materials (SNM) are stored in vaults at several locations on the site. The security infrastructure has been in a state of disrepair. As recently as a few years ago it was found that someone could get inside the fence without being detected because of the poor quality of the closed-circuit TV cameras. Until recently one of the vaults storing SNM even had a window.

The House Subcommittee on Oversight and Investigations was concerned about the security of this site as early as the early 1980's. According to former Chairman John Dingell, "The Subcommittee's work on this matter began in 1981 in response to efforts to undermine independent review of security threats. . .[T]he safeguards at the most critical facilities — which included Los Alamos – were in shambles while, at the same time, DOE's Office of Safeguards and Security was giving the facilities a clean bill of health." (Appendix S)

In 1997, a special unit of the U.S. Army Special Forces was the adversary during a force-on-force exercise. The normal theft scenario is to "steal" enough SNM for a crude nuclear weapon that would fit in rucksacks. But, according to the *Wall Street Journal*, this exercise required that they "steal" more HEU than a person can carry. Not to be outmaneuvered, the Army Special Forces commandos went to Home Depot and bought a garden cart. They attacked TA-18, loaded the garden cart with nuclear materials, and left the facility. "[T]he invaders reached the simulated objective of the game: enough nuclear material to make an atom bomb." And they did so with relative ease. As the *Wall Street Journal* reported,

> "The Garden Cart attackers. . .used snipers hidden in the hills to "kill" the first guards [protective forces] who arrived. Because they happened to be the commanders of the guard force, the rest of the force was thrown into disarray. Many of them also were "killed" as they arrived in small groups down a narrow road leading to TA-18. '[The Special Forces] took them out piecemeal as they came in,' says one participant in the game, whose account wasn't challenged by DOE or lab officials." (Appendix T)

As the *Wall Street Journal* further noted, "The 1997 mock invasion succeeded despite months of guard [protective forces] training and dozens of computerized battle simulations showing that newly beefed-up defenders of the facility would win." (Appendix T)

In 1998, while completing their required annual survey, the Albuquerque Operations Office found the security at TA-18 and other Los Alamos sites unsatisfactory. By the time the report made its way through top management, the unsatisfactory became satisfactory, with no change in actual security. A force-on-force exercise was performed by the 1998 survey team, but they reported that the Los Alamos protective force had compromised the exercise. The DOE Inspector General found that DOE supervisors in Albuquerque refused to investigate the matter. A more detailed description of these incidents is found on pages 28-29 in the Field Operations Office annual surveys section of this report. (Appendix U)

In the Summer of 1999, Secretary Richardson's security team inspected Los Alamos and recommended that TA-18 be shut down and immediately de-inventoried because it could not be defended. However, DOE management persuaded Secretary Richardson not to shut down the site immediately, but instead to further study the matter. In the Fall of 1999, Secretary Richardson created a relocation team to recommend alternative sites for the TA-18 missions. (Appendix V)

In January 2000, while on a site visit to TA-18, members of the relocation team raised questions about an obvious vulnerability at this site. In a semi-hardened building, one of the burst reactors with large plates of HEU fuel was properly stored in an upgraded vault. Another almost identical reactor was sitting in the middle of an open area. The obvious security issue was to either put the reactor in a vault, or take the fuel out and store it in a vault. Los Alamos management refused to do either. (Appendix A)

In a meeting to determine the relocation team's recommendation to Secretary Richardson, Defense Programs (the predecessor organization to the National Nuclear Security Administration [NNSA]) was the lone voice out of ten DOE offices that resisted relocating the facility. Defense Programs took this position in the very memo where they pointed out it would be less expensive to move TA-18 to a more secure site. (Appendix V)

In April 2000, Secretary Richardson, against strong reactions from DOE Defense Programs, ordered that TA-18 be shut down and the SNM completely removed by 2004. He also ordered that a Memorandum of Decision (MOD) be completed by January 15, 2001, in which he would identify the new location for the TA-18 mission. Defense Programs dragged their feet and had barely started the necessary steps to complete the MOD, including the Environmental Impact Statement (EIS) by the deadline. (Appendix X)

In October 2000, the Headquarters Independent Oversight group ran a force-on-force attack – gaining access to the reactor fuel and potentially causing a sizable nuclear detonation that would have taken out part of New Mexico and caused havoc downwind. (Appendix A)

On November 22, 2000, shortly after a meeting with Secretary Richardson, NNSA Director General John Gordon sent an angry letter to Los Alamos Lab Director Dr. John Browne threatening to shut down TA-18 after the debacle in October. Gordon wrote:

> "The failure of the University of California to submit a suitable corrective action plan and to correct in a timely manner the deficiencies cited in an October 2000 assessment of TA-18 security capabilities is unacceptable. As you know, the assessment identified a number of improvements but also several significant weaknesses – most notably in the security strategy, the level of response training, and in the security forces' understanding of appropriate response procedures. **The problems that were noted can be fixed by changes in strategy without the need for the site to incur significant additional costs** (emphasis added). . .If any of these actions do not occur, all activities at TA-18 will be immediately suspended until the actions have been taken and verified." (Appendix Y)

A DOE Headquarters security team went to Los Alamos in December of 2000 to verify that Los Alamos had made adequate upgrades. While they had made upgrades, the changes had not been performance tested to ascertain their effectiveness. An internal DOE memorandum raised basic questions about the adequacy of the "new and improved" protection of this site. (Appendix A)

Transportation Security Division

The Department of Energy Transportation Security Division (TSD) moves nuclear weapons, as well as weapons-grade uranium and plutonium, from site to site across the nation on public highways. The protective forces in the Transportation Division are civilian federal employees. In late 1998, TSD submitted a Site Safeguards and Security Plan (SSSP) to Headquarters for approval. Preliminary examination of the testing scenarios revealed that the SSSP used simplistic attacks and "dumbed down" use of weapons.

During planning phases the TSD team of specialists and commanders were aghast at the proposed use of sniper rifles with armor-piercing incendiary rounds by the adversaries. The DOE Inspector General determined that DOE management considered the use of a sniper rifle unreasonable and that only "super adversaries" would use them. In fact, these weapons have been available since World War I. The GAO found in an undercover investigation that more than 100,000 rounds of Pentagon-surplus armor-piercing incendiary rounds have been sold on the civilian market. (Appendix Z)

At the DOE Pantex nuclear weapons-assembly facility, security officials believed that armored Humvees were death traps, because of the availability of armor-piercing incendiary rounds. The Pantex Security Director lamented that he would never allow his protective forces to fight from them, and that it would have been just as effective to buy Yugo's. Incredibly, the next day, Secretary Richardson's security team was at Sandia, and found officials in the process of

buying armored Humvees. Using these readily-available armor-piercing incendiary rounds, terrorists could shoot through the armored truck cabs, killing the driver and protective forces, making the transported nuclear materials ready for the taking.

In the simulation phase only four tests were run. According to sources familiar with the test, the TSD protective forces were literally annihilated in tens of seconds after an attack was started. In after-action briefings the convoy commander admitted that they had experienced similar results in force-on-force testing many months earlier. Part of the problem was that the guards' weapons were of inadequate range to reach the adversary.

A December 12, 1998 internal DOE memorandum reported on the computerized Joint Tactical Simulations (JTS) evaluations of the Transportation Division's SSSP conducted at Sandia: "JTS results on the first worst case scenario. . .were 3 losses and no wins. JTS results on the second worst case scenario. . .were 3 losses and 1 win. The high TSD JTS loss rate for the first two worst case scenarios caused TSD to request termination of JTS activity. TSD requested DOE Headquarters' assistance to analyze the poor results and begin to determine possible corrective actions." (Appendix B)

In early 1999, a special force-on-force test was run at Fort Hood for the luminaries from Washington – Deputy Secretary, Undersecretary and top security and program officials, to show that the TSD could handle the threat. The U.S. Army Special Forces provided the adversaries. The protective force won. However, according to a Special Forces representative, he noticed a piece of paper held by a protective force member that he had just "shot" – it was a complete outline of the mock terrorists' attack plan. The protective force was cheating. Secretary Richardson's Special Assistant, Peter Stockton, proved the cheating to the Albuquerque manager and the TSD manager. No action was taken. (Appendix W)

In November 1999, an Army Special Forces representative found that the new sniper rifles used by TSD were target range variety, not for combat in rugged terrain. In fact, the sights on the rifles were very sensitive and would not survive the rigors of combat. More than half of the unclassified recommendations made by the DOE Inspector General regarding the SSSP process were focused on improving the security of the TSD program. (Appendix MM)

Major Threats to the Complex

There are four particularly worrisome threats that cut across the complex: 1. The threat of attack by weapons of mass destruction; 2. The threat of truck bombs; 3. The threat of the creation of an Improvised Nuclear Device from the material at particular DOE sites; and 4.The threat of theft of nuclear secrets.

Weapons of Mass Destruction

In the summer of 1995, then-President Clinton issued Presidential Decision Directive 39 (PDD-39) to address the nation's concern over the use of weapons of mass destruction (WMD) against our citizens.[11] Weapons of mass destruction are biological, chemical, radiological, and nuclear. In May of 1998 he added a supplemental directive PDD-62 reaffirming PDD-39. These two directives "highlight the growing threat of unconventional attacks against the United States," including, "terrorist attacks, use of weapons of mass destruction, assaults on our critical infrastructures and cyber-attacks." [12]

The use of chemical and biological weapons has barely reached the level of consciousness in DOE. Security tests at the facilities do not include weapons of mass destruction in their scenarios. Chemical and biological weapons are not even considered in the Site Safeguards and Security Plans or SSSPs at any of the DOE nuclear sites. Keep in mind the use of chemical or biological weapons against DOE weapons facilities is as a limited engagement device for the terrorist to neutralize the protective forces and gain access to the SNM on site for theft, creation of an Improvised Nuclear Device (IND), or radiological dispersal sabotage. In a recent force-on-force drill at Los Alamos, the adversary force used a simulated irritant gas against the protective force. The protective force was totally unprepared for even the use of the gas mask. (Appendix A)

Five and a half years after PDD-39 was issued by President Clinton, DOE now has a classified study underway on developing strategies against chemical and biological attacks. It is believed that this study will recommend further study.

---

[11] Official policy positions by the President of the United States are issued through the National Security Council in the form of Presidential Decision Directives (PDD).

[12] http://www.info-sec.com/ciao/6263summary.html – Downloaded on September 14, 2001.

Truck Bombs

Since the U.S. Marine barracks in Beirut, Lebanon, were leveled by a truck bomb in 1983, DOE facilities have been required to protect against truck bombs. The U.S. Government has suffered significantly from truck bombs:

- U.S. Embassy in Beirut, Lebanon on April 18, 1983;
- U.S. Marine barracks in Beirut, Lebanon on October 23, 1983;
- U.S. Embassy in Kuwait on December 12, 1983;
- World Trade Center in New York City on February 26, 1993;
- The Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995;
- Khobar Towers in Dhahran, Saudi Arabia on June 25, 1996;
- U.S. Embassies in Nairobi, Kenya and Dar es Salaam, Tanzania on August 7, 1998; and
- USS Cole Naval Destroyer in Yemen (a rubber boat bomb) on October 12, 2000.

A September 2000 CIA Interagency Intelligence Committee on Terrorism report points out, "These massive vehicular bombs have illustrated the need for substantial vehicle access denial systems to afford a buffer area between bomb vehicle and the building or facility requiring protection." (Appendix AA)

A truck bomb at a nuclear weapons plant could be devastating, dispersing tons of PU or HEU over the surrounding communities. As discussed on page 14, Secretary Richardson's security team found that Rocky Flats was vulnerable to such an attack. They had placed the vehicle barrier cable on the outside fence rather than the inside fence. A terrorist could have cut the cable on the outside fence (which does not have alarms), driven a large truck through both fences and up against the wall of a vault containing tons of PU, and detonate a bomb before any credible response could be mounted by the protective force. Putting the cable on the inside fence would slow down an intruder once they have already broken through the outside fence, and set off the sensors between the fences thereby alerting protective forces to their presence. This is 16 years after the bombing of the U.S. Marine barracks in Beirut, 4 years after the Presidential Decision Directive on terrorism, and 2-1/2 years after this was initially discovered and Rocky Flats was ordered to fix it.

At the Pantex Plant during one of the Secretary's Special Assistant's visits in 1999 it was noted that the vehicle barrier on the primary road into the main storage area was installed backwards. Instead of stopping a vehicle the barrier would provide a ramp for the vehicle to drive over. Pantex, is the crown of DOE, and this area was the jewel in that crown. This area had been inspected and examined countless times by the assessment, survey and inspection groups since 1995.

The Creation of an Improvised Nuclear Device

A Improvised Nuclear Device (IND) explosion is qualitatively different from exploding SNMs with a homemade bomb. While exploding PU or HEU with a bomb would cause a major dispersion of highly radioactive materials as occurred at the Chernobyl Reactor in the Ukraine, an IND explosion could cause a chain reaction on par with the devastation of Hiroshima and Nagasaki, Japan. An IND can be created at a number of DOE sites because of the presence of nuclear weapons or special nuclear materials in bomb grade quality and quantity. This can cause nuclear detonations of varying sizes. Little time is required to accomplish this act. In a force-on-force test in October 2000 at TA-18, at Los Alamos, the protective force failed to stop the "terrorists" from gaining access – therefore a sizable nuclear detonation was possible. (Appendix BB)

Frighteningly, a terrorist group would not have to steal nuclear material, create a nuclear device, transport it in a suitcase to the United States, and detonate it in a major city. They could simply gain access to the material at a U.S. nuclear facility, some of which are near large cities where they could accomplish the same outcome. As the former DOE Director of Office of Safeguards and Security simply stated regarding Rocky Flats, ". . .you don't need to take it in the middle of Denver, it's going in the middle of Denver anyway." (Appendix O)

Although discussing the potential for an IND explosion is not classified, discussing the details of how such an explosion could be detonated has been classified by DOE as a Special Access Program (SAP). This vulnerability is widely recognized within the defense community, however DOE takes the stance that analyzing and fixing this vulnerability cannot be discussed by anyone other than those in the small "club" who have clearance for the SAP program. As a result, security experts have been forced to wait for these people to address this problem – and they have been waiting for decades.

Theft of Nuclear Secrets

In early 1999, the Los Alamos cyber security failures surprised DOE. Congress and the press were highly critical of DOE for its inability to protect classified information on their computer systems. The Rudman Panel bemoaned the constant use of ineffective commissions and panels to review ongoing security failures at DOE:

> "Management and security problems have recurred so frequently that they have resulted in nonstop reform initiatives, external reviews, and changes in policy directions. . . . During that time, security and counterintelligence responsibilities have been 'punted' from one office to the next. . . .Particularly egregious have been the failures to enforce cyber-security measures to protect and control important nuclear weapons design information. Never before has the panel found an agency with the bureaucratic insolence to dispute, delay, and resist

> implementation of a Presidential directive on security, as DOE's bureaucracy tried to do to the Presidential Decision Directive No. 61 in February 1998."[13]

DOE's answer to this crisis was to initiate yet another multi-million dollar commission to study the matter. In the Fall of 1999, DOE's Defense Programs presented a foot-thick report entitled "Information Security Management" to the Undersecretary with a $1.3 billion price tag to solve the problem. Obviously it was not funded due to budgetary constraints. In the Summer of 2000, an internal review of cyber security of classified information found DOE had done nothing effective to stop a trusted insider from downloading the Mother Lode (bomb design information, etc.) and walking out the door – exactly the concerns raised at Los Alamos eighteen months earlier.[14] (Appendix D)

The major threat to the compromise of critical information at DOE is the "insider" – trusted employees. Virtually all of our known spies have been "insiders" with the highest security clearances. The DOE security team reviewed many of the interagency threat documents – all came to the same conclusion – the "insider" is a priority problem. Despite this, the vast majority of planning and preparations was aimed at protecting sensitive information from "outsiders."[15] (Appendix D)

A number of experts believe that there are ways of protecting priority information to near certainty for very little money – but it just doesn't happen. The Labs simply refuse to prioritize what should be protected because they are more concerned about convenience for the scientists rather than security. The Warren Rudman lead President's Foreign Intelligence Advisory Board (PFIAB) Panel concluded:

> ". . . many officials interviewed by the PFIAB panel cited the scientific culture of the weapons laboratories as a factor that complicates, perhaps even undermines, the ability of the Department to consistently implement its security procedures. . . . The prevailing culture of the weapons labs is widely perceived as contributing to security and counterintelligence problems."[16]

There is a device that looks like a child's Game Boy that can download the equivalent of 1100 floppy disks off a computer in 3 minutes and 14 seconds. There is also a device called a memory stick about the size of a stick of gum that can hold the equivalent of 44 floppy disks. Virtually the only way to stop the abuse of this technology is the use of "media-less" computing. To stop an "insider" you have to stop any media (disks, tapes, laptops, etc.) from coming in or going out of priority classified areas. On August 30-31, 2000, a meeting was held at Lawrence

---

[13] http://fas.org/sgp/library/pfiab/ – Downloaded September 13, 2001.

[14] Ibid.

[15] Ibid.

[16] Ibid.

Livermore with the Chief Information Officers of the key facilities and labs and the DOE officials from the Operations Offices. Everyone agreed that DOE had to move ahead quickly on the "insider" problem before the Hill or the press found out that virtually nothing effective had been done to stop a dedicated insider. (Appendix D; Appendix CC)

An implementation strategy was established at the Livermore meeting for near-term enhanced security for classified systems including implementing "media-less" computing systems. (Appendix CC) A schedule was developed during this meeting that would have had this system in place before the end of 2000 at a cost in the neighborhood of $10-15 million. The consensus was that these changes would have taken DOE from a low confidence level that a trusted insider could be stopped, to near certainty.

The effort was rejected by the NNSA representative, John Todd, in deference to the alleged functionality and morale concerns of the lab scientists. In the battle between morale of scientists and security, security always loses. In an October 30, 2000 memo to then-DOE Secretary Richardson, his Special Assistant Peter Stockton wrote,

> " . . .Todd argued that this effort should be delayed because it may have a negative impact on lab morale. Todd's solution was to install lock boxes like those he was implementing at Naval Reactors. He admitted that the lock boxes were not effective against a dedicated insider, and they would not increase security, but they would increase functionality for the scientists – they could leave their computers on when they left their offices. I visited Naval Reactors and met with their security officials to discuss their experience with lock boxes. They admitted that they would not be effective against the dedicated insider, and that they had obvious vulnerabilities. . .This is again based on the wants of the scientists rather than the real security needs of the system." (Appendix D)

Misleading Test Results – And they Still Lose 50% of the Time

Dumbed-down Security Tests

Past results have demonstrated that security forces and DOE field management have learned how to "game-the-game" to the extent that most tests are unrealistic, tactics are "canned" and expected, and the outcome of exercises are pre-ordained. Two techniques are used to performance test the protection system effectiveness – 1) force-on-force tests performed by mock terrorists from the DOE, Army Special Forces and Navy SEALs, and 2) computerized Joint Tactical Simulations (JTS).

A number of groups including the Army Special Forces, Special Operations Unit of the Special Forces, the Navy SEALs and DOE's Office of Independent Oversight have raised serious questions about realism of the force-on-force tests and the JTS computer simulations used to test

the effectiveness of protective force responses. They all argue that exercise artificialities make the protective forces appear far more capable than they actually are – yet even with the scales tipped in their direction, protective forces still lose over 50% of the time. (Appendix DD)

The protective forces are civilian private contractors not under military discipline or the military command structure. A postulated terrorist attack on these facilities would be not only a surprise but also extraordinarily violent, considering the conventional weaponry and explosives available to terrorists today. Some experts question whether the protective forces would have the training or experience or would continue to fight under these circumstances. It is not a question of the personal courage or dedication of the protective force, but the daunting circumstances under which they are placed by the system.

On August 30, 1999, the DOE Office of Independent Oversight sent an unusually candid memorandum marked "For Official Use Only" to the new security czar, describing in detail the weaknesses and artificialities of the security testing process at DOE. According to this office:

> "The. . .more serious concern pertains to the actual content and quality of the VAs [Vulnerability Analyses] that support the current SSSPs. This issue, which calls into question the very foundation of the risk calculations used throughout the Department, has received little attention from safeguards and security managers. It is this concern that forms the subject of this paper. . .
>
> **"There Are Significant Errors in the Database Supporting the JTS Combat Simulation Model.** . . .In addition to the identified errors, a significant number of readily available weapons and munition types are not included in the database. . .
>
> **"Adversary Tactics Are Poorly Thought-Out.** Observed adversary tactics used during JTS simulations and validation and verification force-on-force tests are frequently crude, and often do not rise to the level expected of troops who have completed basic infantry training. . .Personnel assigned to portray adversaries in modeling and performance testing are generally given only a few days to prepare tactical plans. A special problem with JTS simulations is that, generally, one computer operator is assigned to control the entire adversary team, while three (sometimes more) operators are employed to represent the protective force. This leads to situations where one adversary element is well managed in the simulation, while other elements are neglected and relatively ineffective. . .
>
> **"Currently, no one in DOE outside of the Office of Safeguards and Security Evaluations [of the Office of Independent Oversight] appears to have a consistent interest in either cultivating the adversary mind-set or an understanding of adversary capabilities."** [Emphasis added] (Appendix I)

This document clearly articulates the grave concerns of the DOE Independent Oversight Office regarding the inadequacies of the simulation and exercise test system used by DOE, and its inability to accurately predict security capability or status.

There is virtually no surprise in a force-on-force test. Once the protective force is outfitted with the Multiple Integrated Laser Engagement System (MILES) weapons laser-simulation equipment, they know the attack will take place within an hour or two. The specific location of the attack is always tipped off by the controllers and the observers during the "safety walk down." A walk down is performed across the whole area where a battle will be simulated to ensure no obstacles or other land variations would trip or otherwise injure the protective forces during the exercise – obviously not creating a realistic scenario. This is far more than leaning forward in the foxhole.

Another indicator of the artificiality of force-on-forces' are the baffling reactions of the protective forces during the tests. For example, in the force-on-force test at Rocky Flats in 1998, 1999 and again in 2000, the protective force "indiscriminately shot" scientists, controlling referees in orange vests, and each other as they were exiting the building in response to the alarm.

> "Two Multiple Integrated Laser Engagement System (MILES) enhanced exercises were observed where protective force members 'killed' building evacuees, controllers wearing orange safety vests, and each other. During the critique conducted immediately after the exercise, protective force and other site management personnel failed to raise concerns related to the inappropriate use of deadly force. In fact, no critical observations were surfaced by management at the critique. . .In law enforcement training environments, the typical 'penalty' for killing a 'friendly' is failure of the test. At RF [Rocky Flats], there are currently no negative consequences for the inappropriate use of deadly force. In fact, if the adversaries are 'killed' in the process, the result is actually a win from the site's current perspective. This situation is unacceptable and must be addressed immediately." (Appendix C)

This obviously is not a realistic demonstration of how the protective forces would react to a terrorist attack, making the force-on-force test next to useless. DOE Headquarters had already warned Rocky Flats about this inappropriate use of deadly force.

During the March 2000 force-on-force drill, extreme restrictions were placed on the adversaries by Rocky Flats management. The commando adversary team was prohibited from using their own radios and "could not effectively communicate." In addition, the commandoes were not even allowed to drive around a road block "simulated by a PF [protective force] vehicle being parked on the side of the road and a traffic cone placed in the center of the road," which led to the facility. To suggest terrorists would not drive around a car and traffic cone to reach their target stretches reasonable expectations. (Appendix C)

In a force-on-force test at Los Alamos in October 2000, a convoy of protective forces responding to an attack at another site hit a "minefield." Despite the fact that the first vehicle hit a mine and would have been destroyed, the other vehicles continued on through the minefield. Military doctrine and common sense clearly calls for a convoy to stop when hitting a minefield. Los Alamos management's response was that they didn't have time to stop. (Appendix A)

Overstatement of Protective Force Combat Effectiveness

A recent force-on-force test illustrates the problem of combat ineffectiveness. In a memo to then-Energy Secretary Richardson his Special Assistant Peter Stockton wrote, "[D]espite the absolutely critical requirement for "denial" [not allowing an adversary in a building]. . .denial failed." It is clear that if denial were to fail in a real attack, such a facility cannot be recaptured because of the extraordinary percentage of protective forces killed in the initial skirmish. Military doctrine dictates when losses exceed 20%, forces become combat ineffective due to loss of command and communications and basic squad-sized tactics deficiencies. In this force-on-force test, the site lost 50% of their protective force in the initial attack – with eight dead on the doorstep of the facility. At this point, according to combat veterans, there would likely be no further offensive action to recapture the facility by the protective force. In a number of force-on-force scenarios developed by DOE, even when the protective force is successful in repelling an attack, they lose up to 80-95% of the force. This is simply unrealistic. Los Alamos security officials admit this is a problem, but they claim they have unusually brave people. Real bullets may make a difference in their calculation. As an Army Special Forces Commander wrote:

> "As a unit sustains casualties (dead or wounded) elements of the fire and maneuver schemes or 'close quarter battle' drills begin to come apart. . . .[I]f casualties are high (in excess of 10%) qualified replacements become increasingly problematic and command and control begins to be lost. Units are normally considered "combat ineffective" and are rotated off the line when they have sustained 15-20% casualties. At this point maneuver, fire rates, communications and command and control can no longer be relied on to support the mission. Continuation would be expected to result in unnecessary and increasingly high casualties with little expectation of success." (Appendix A)

The clear solution is to shut down sites that can't be protected; if they have a critical mission, move sensitive materials to a site that can be protected.

Simple "access denial systems" are available to the U.S. government which would delay terrorist access to sensitive materials. These systems were developed by DOE and are currently deployed at DOD facilities but not at DOE.

Security analysts claim that Protective Forces are not robust in tactics, weaponry or numbers and result in a low probability of success – all of which results in force-on-force failures in more than 50% of the tests. (Appendix DD) Even with improved tactics and weaponry, the

protective force at the 10 critical fixed DOE sites are still at half the manpower level deployed in 1992.

Naturally, safety is a constant concern for all DOE employees. However, the same safety standards that apply to an office worker also apply to the protective force. Because of this universal application of safety standards the protective forces are encouraged not to, and in many cases prohibited from, engaging in any activity that could possibly result in **any** injury. All this contributes to a protective force unable and unwilling to respond when they are most needed.

Security Oversight – A Weak Record

In Congressional testimony, DOE has led the public to believe that its security at these sites is a well-oiled machine, and there is nothing to worry about. After all, they argue the government has been building bombs at these sites for 60 years, and no one has attacked them yet. Given the recent tragedies in New York and Washington, DC, this argument falls flat. In fact, they are one-eyed toothless watchdogs. Each level of oversight fails for varying reasons: conflict of interest, protection of the contractor, embarrassment, protection of the program, political sensitivities, and bureaucratic survival. The following is an analysis up the chain of command of this "redundant" security oversight apparatus:

Up the Security Chain of Command

➢ *Contractor self-assessments* are a basic conflict of interest. It is not in the interest of the contractor to reveal problems which could lead to further investigation and a cut in their performance bonuses and award fees. The Inspector General (IG or OIG) recently found in interviews that most of the employees performing contractor self-assessments felt they were under pressure from the contractor not to find problems:

> "[T]he OIG found that 8 of the 28 LANL Security Operations Division personnel interviewed (approximately 30 percent) who had conducted self-assessments believed they had been pressured to change or "mitigate" security self-assessments. Several of these individuals said LANL management appeared to be more concerned about making LANL and the Security Operations Division "look good" than reporting the actual security conditions at LANL. The OIG was informed of two instances where LANL management became so upset with issues raised by the initially assigned reviewers, that management reassigned other reviewers who subsequently determined that there were no issues to be raised and that the organizations were satisfactory." (Appendix U)

The IG also found that Los Alamos National Lab (LANL) had been paid by the government for self-assessments that were not done: "In addition to finding that some

self-assessments were not conducted, the OIG also found an instance where a self-assessment report was written without a self-assessment review being conducted." (Appendix U)

- *Federal Area Offices* – The DOE Inspector General found the Los Alamos Area Office not technically capable of performing their security oversight function. "Several DOE personnel told us that LAAO [Los Alamos Area Office] security was understaffed and did not have the technical expertise required to conduct all their oversight responsibilities." (Appendix U)

- *Field Operations Office annual surveys* – During the 1998 Albuquerque annual survey reviewing security at Los Alamos (LANL), it was determined that security was unsatisfactory or marginal in most categories. By the time the report journeyed through the political review process at the Field Office, the ratings were substantially improved – most to satisfactory. The IG found there was no written justification for the change, and in fact, a number of key documents necessary to justify such changes in ratings had been destroyed:

> "During the 1998 Albuquerque Security Survey at LANL, Albuquerque management upgraded several topic area survey ratings, and most importantly, the overall composite rating. . . During our inspection we noted that the 1997 and some 1998 Albuquerque Security Survey work papers were destroyed . . . As a result, there was no complete record to show how the survey teams developed the ratings." (Appendix U)

In addition, the IG reported that during the same 1998 annual survey, a force-on-force exercise was reported to have been compromised – or rigged. One of the force-on-force mock terrorists reported the compromise, as well as his concerns regarding the Protective Force response, to the Albuquerque Field Office. According to the IG, "Albuquerque [Field Office] management did not fully assess concerns" about the incident, yet that office boldly stated "there was no evidence of 'cheating' and that 'the losers always complain that the winner cheated." The IG reported:

> ". . . [H]ad the compromise of the force-on-force exercise been included in the 1998 Albuquerque Security Survey report, the composite rating would have been 'unsatisfactory'. Instead LANL was given a 'marginal' rating." (Appendix U)

The following Inspector General chart reveals the changes made by the Field Operations Office management from ratings of "unsatisfactory" to ratings of "marginal" or "satisfactory":

Appendix C

1998 Security Survey Rating Changes[11]

Program Topic Areas:	Team Leader	Murder board	Final Report
Program Management			
Program Management and Administration	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Program Planning	Satisfactory	Satisfactory	Satisfactory
Personnel Development and Training	Satisfactory	Satisfactory	Satisfactory
Facility Approval and Registration of Activities	Satisfactory	Satisfactory	Satisfactory
Foreign Ownership, Control, or Influence	Satisfactory	Satisfactory	Satisfactory
Safeguards and Security Plans	Unsatisfactory	Unsatisfactory	Unsatisfactory
Surveys and Self Assessment	Satisfactory	Satisfactory	Satisfactory
Resolution of Findings	**Satisfactory**	**Marginal**	**Satisfactory**
Incident Reporting and Management	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	Unsatisfactory	Unsatisfactory	Marginal
Protection Program Operations			
Physical Security	Marginal	Marginal	Marginal
Security Systems	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Protective Force	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Security Badges, Credentials and Shields	Satisfactory	Satisfactory	Satisfactory
Transportation Security	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	Unsatisfactory	Unsatisfactory	Marginal
Information Security			
Classified Guidance	Satisfactory	Satisfactory	Satisfactory
Classified Matter Protection and Control	**Satisfactory**	**Marginal**	**Marginal**
Special Access Programs and Intelligence Information	Satisfactory	Satisfactory	Satisfactory
Classified Automated Information Systems Security	Satisfactory	Satisfactory	Satisfactory
Technical Surveillance Countermeasures	Satisfactory	Satisfactory	Satisfactory
Operations Security	Satisfactory	Satisfactory	Satisfactory
Unclassified AISS (Optional)	Unsatisfactory	Unsatisfactory	Unsatisfactory
Protected Distribution System (Optional)	Satisfactory	Satisfactory	Satisfactory
Communications Security (COMSEC) (Optional	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	Marginal	Marginal	Marginal
Nuclear Materials Control and Accountability			
Basic Requirements	**Marginal**	**Unsatisfactory**	**Marginal**
Material Accounting	Unsatisfactory	Unsatisfactory	Unsatisfactory
Material Control	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
OVERALL RATING	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Personnel Security			
Access Authorization (Personnel Clearance)	Satisfactory	Satisfactory	Satisfactory
Security Education Briefings and Awareness	Satisfactory	Satisfactory	Satisfactory
Control of Visits	Satisfactory	Satisfactory	Satisfactory
Unclassified visits and Assign by Foreign Nationals	**Satisfactory**	**Marginal**	**Satisfactory**
Personnel Assurance Program	Satisfactory	Satisfactory	Satisfactory
Personnel Security Assurance Program	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory	Satisfactory
1998 Composite Rating	**Unsatisfactory**	**Unsatisfactory**	**Marginal**

Items in **Bold** indicate changes in ratings.

[11] There is no documentation for the 1999 Security Survey that provides a similar Team Leader rating breakdown.

- *The Office of Independent Oversight* reports directly to the Secretary of Energy. This office is a qualified and capable group. Their 1999 memo to the security czar, quoted extensively on pages 10 and 24 details their strong analysis and urgent concerns regarding DOE security. However they are in a position not only to take direction from the Secretary but also to play to perceived political sensitivities. It takes a high wire act to survive in this position. Rarely does it serve the political purposes of the Secretary to have documented and potentially embarrassing security problems surfacing that could be discovered by Congress or the press. There are instances where this oversight group has pulled punches or simply not tested certain sites, knowing they would fail at a politically sensitive time. A draft December 1999 GAO report entitled, "Nuclear Security: Improvements Needed in DOE's Safeguards and Security Oversight" revealed that "The director of OSSE [Office of Safeguards and Security Evaluations, DOE Independent Oversight] informed us [the GAO] that inspections were not conducted annually from 1994 through 1998 because Secretarial interest in the safeguards and security area waned and staff allocated for safeguards and security inspections was reduced." (Appendix EE)

The following draft GAO table shows the conflicts between the security ratings given by the Office of Independent Oversight (referred to in chart as OSSE), DOE Field Operations Offices, contractor performance evaluations, and the final reports to the President:

Table 1: Safeguards and Security Ratings for Los Alamos National Laboratory From 1994 through 1999.

Year	OSSE	Operations Office	Contract Performance	Report to the President
1994	No rating given	Marginal	Exceeds expectations	Marginal
1995	Inspection not conducted	Satisfactory	Far exceeds expectations	Satisfactory
1996	Inspection not conducted	Survey not conducted	Far exceeds expectations	Satisfactory
1997	No rating given	Marginal	Meets Expectations	Report not issued
1998	No rating given	Marginal	Excellent	Marginal
1999	Satisfactory	Marginal	To be determined	To be determined

Table 2: Safeguards and Security Ratings for Lawrence Livermore National Laboratory From 1994 through 1999.

Year	OSSE	Operations Office	Contract Performance	Report to the President
1994	Inspection not conducted	Survey not conducted	Excellent	Satisfactory
1995	Inspection not conducted	Satisfactory	Far exceeds expectations	Satisfactory
1996	Inspection not conducted	Satisfactory	Far exceeds expectations	Marginal
1997	No rating given	Satisfactory	Far exceeds Expectations	Report not issued
1998	No rating given	Marginal	Good	Marginal
1999	Marginal	Marginal	To be determined	To be determined

DRAFT

➢ *Reports to the President on the Status of Safeguards and Security at DOE* were produced annually by the Office of Safeguards and Security (OSS). Back in the 1980's Chairman Dingell found DOE misleading the President and the National Security Council about the status of security in these reports. In 1996, a critical report was drafted by the Director of OSS, Edward McCallum, but not released by DOE to the President. Finally, the National Security Council demanded its release. Shortly thereafter, McCallum was then put on administrative leave and investigated. The investigation was later dropped. The next year, no report was issued. (Appendix L; Appendix FF)

National Nuclear Security Administration
Different Name, Same Problem

In the wake of the Los Alamos security breach, the Congress reacted by legislatively mandating the reorganization of the nuclear weapons program in DOE by creating a semi-autonomous agency reporting to the Secretary – National Nuclear Security Administration (NNSA). Even though the Agency was named the National Nuclear **Security** Administration, security is only one of the many duties entrusted to it.

For example, on June 27, 2001, Administrator of the National Nuclear Security Administration General Gordon testified before the House Armed Services Committee on the work and budget needs of the NNSA. Out of 44 single-spaced pages of testimony, General Gordon only devoted 1 ½ pages to physical and cyber security. This testimony demonstrates the extraordinary span of General Gordon's responsibilities: there is no way security (and safety for that matter) can compete with nuclear submarines, non-proliferation deals with Russia, and stockpile surety. This hodgepodge is clearly, as General Gordon says, "fragile" if not worse.[17]

The Los Alamos case was a cyber security problem and an alleged counter intelligence issue. There have been no hearings since the early 1990's addressing the myriad of issues involved in physical security. The reorganization did nothing to address the physical security problems. In fact it exacerbated the problems. It was simply a rearrangement of the deck chairs in a bureaucracy that has failed. In a memo from NNSA's Principle Deputy Administrator, Bob Kuckuck even stated, "This reorganization is predominantly a functional realignment – with many employees continuing to perform their current functions." He went on to say that many employees would even "continue to report to their current supervisor." (Appendix GG) Furthermore, several of the new appointments to top NNSA positions were the very same people who oversaw the agency's predecessor, DOE Defense Programs. At that time, Representative John Dingell (D-MI) warned that this was a mistake:

> "I am gravely concerned about recent proposals to elevate the Department's dysfunctional weapons bureaucracy to the status of an almost completely autonomous agency. . .We are concerned that the same bureaucrats, who have

[17] http://www.nnsa.doe.gov/docs/JAG_HASC_Testimony_6-27.pdf – Downloaded September 13, 2001.

refused to implement President Clinton's recent security order and who resisted reform efforts by both the Bush and Clinton Administrations, would be running this agency, with even greater latitude and far less oversight than is currently in place. **Allowing these proposals to become law would be tantamount to using gasoline to extinguish a fire. . .This would indeed be a remarkable act of political jujitsu where the very institutions responsible for the security problems at DOE would emerge from scandal not merely intact, but even more powerful and autonomous than before.**" (Emphasis added) (Appendix S)

As it has turned out, the Congress has already realized they simply created another unwieldy bureaucracy. In the FY2002 House Appropriations Report, it was observed that, "Congress assumed that creation of the NNSA would lead to efficiencies and streamlined management. However, the result has been an increase in staff at Headquarters and in the field." (Appendix HH)

Lack of Congressional Oversight

In testimony before the House Commerce Committee on April 20, 1999, the GAO stated "we are concerned that, given DOE's past record, it may not be up to the challenge without congressional oversight to hold it accountable for achieving specific goals and objectives for security reform." (Appendix II)

There are two things that move any bureaucracy: one is sustained press attention to a problem and second is congressional oversight. For example, recently there was sustained press attention to the plutonium contamination of workers at a DOE facility at Paducah, Kentucky which finally lead DOE to compensate the injured workers and their families. Over the last 20-30 years, there has never been sustained press attention paid to security debacles at DOE because the Department has been able to hide behind overclassification.

Throughout the 1980's and early 1990's, Chairman John Dingell (D-MI) of the House Energy and Commerce Committee conducted numerous investigations of security lapses. One major problem that Chairman Dingell faced was that he did not have clear jurisdiction over the budget of the nuclear weapons program. He was unable, therefore, to use the most effective threat to the Department – budget cuts.

Despite the efforts of both the GAO and Representative Dingell's Committee, the DOE bureaucracy remained entrenched. According to the President's Foreign Intelligence Advisory Board, "The panel has found that DOE and the weapons laboratories have a deeply rooted culture of low regard for and, at times, hostility to security issues, which has continually frustrated the efforts of its internal and external critics, notably the GAO and House Energy and Commerce Committee."[18]

[18] http://fas.org/sgp/library/pfiab/ – Downloaded September 13, 2001.

The Congressional hearings spurred by the Los Alamos cyber security breaches focused on two specific incidents of security failures, but did not deal with the systemic physical and cyber security problems at the nuclear weapons complex. As this report illustrates, without sustained and intensive scrutiny and oversight, DOE briefings and testimony will not reveal the actual status of security.

Rewards and Punishment Turned On Its Head

Promotions for Security Failures

Whenever a security crisis occurs at DOE, the Secretary usually assures the Congress and the press that the responsible officials will be held accountable. It virtually never happens. As the Rudman report points out, "the lack of accountability . . . has become endemic throughout the entire Department."[19] On the other hand, if someone internally raises an issue about security, they are always retaliated against and find themselves without any further security responsibilities. In other words, the reward and punishment system is turned on its head.

For example, Dr. John Browne, the lab director at Los Alamos, was in charge during the Wen Ho Lee case, the hard drive debacle and the force-on-force in October 2000 that would have led to a nuclear detonation. He is still the lab director. Steve Younger, the head of the X Division at Los Alamos where these debacles took place remained in his job, until appointed by President Bush to become the head of the Pentagon's Defense Threat Reduction Agency. The security director at Los Alamos, Stan Busbaum, is still in his job.

Rocky Flats, which is operated by contractor Kaiser-Hill, had severe security problems in the 1996-98 time frame and again in 1999. In 1997, outgoing Secretary of Energy Hazel O'Leary became a paid Director of Kaiser and outgoing DOE Assistant Secretary for Environmental Management (overseeing Rocky Flats) Tom Grumbly became Senior Vice President for Kaiser. The current DOE Undersecretary Robert Card was President and CEO of the Kaiser-Hill Company. The DOE Manager of the Rocky Flats Field Office from 1996 to 1999, Jessie Roberson, is now the DOE Assistant Secretary for Environmental Management.

The head of the DOE Office of Security Affairs, Joe Mahaley, who was responsible for security at all the sites, and whose office was involved in many of the following retaliations, was promoted to becoming the new security czar.

[19] Ibid.

Whistleblowers: Shooting the Messenger

"In every investigation concerning problems at the DOE weapons facilities and laboratories, the individuals responsible for the operation of defense programs consistently and repeatedly denied the problems, punished the whistle blowers, and covered up the problems to their superiors and Congress."

Representative John D. Dingell (D-MI) (Appendix S)

Retaliation at DOE does not necessarily entail attempting to fire federal employees. In the majority of cases in the security area, DOE supervisors attempt to revoke the whistleblower's clearance on trumped-up charges. Then they remove them from any responsibility for oversight of security. On the other hand, contractors often lose their contracts, or their jobs, for blowing the whistle. The frequency of retaliation against nuclear security whistleblowers reached such a crescendo, that in 1999 then-Secretary Richardson sent a memorandum to all DOE and contract employees stating: "Management must also create and foster a work environment that allows free and open expression of security concerns, where workers fear no reprisals or retaliation." (Appendix JJ)

Over the last three years, in the face of Richardson's "zero-tolerance" of retaliation against security whistleblowers, DOE still succeeded in eliminating all of the whistleblowers, or "speed bumps" in the road, as one federal official put it. In fact, months after this "zero-tolerance" policy was in effect, when the DOE Inspector General was investigating security failures at Los Alamos, "a number of individuals requested confidentiality. They indicated they feared retaliation for disclosing information to the Office of Inspector General." (Appendix U) Currently, there are few DOE employees left in the bureaucracy with the knowledge or willingness to risk the damage to their careers to raise concerns about the lack of security. Retaliation against whistleblowers has been a clear object lesson to the rest of the bureaucracy.

Going back to the early 1980's, there has been a pattern of retaliation against federal and contractor employees who raise issues about security problems. For example:

- In 1980, DOE did not like the fact that John Hanatio, a security analyst at DOE Headquarters, was cooperating with the House Subcommittee on Oversight and Investigations. They immediately went after his security clearance and tried to fire him. Under Subcommittee Chairman John Dingell's (D-MI) protection he is still employed by DOE but has never been placed in a position of significant responsibility or dealt with security issues again.

- In 1996, Colonel David Ridenour, a former Strategic Air Command missile officer, became the Director of the Safeguard and Security Division at the Rocky Flats Field Office. Immediately upon taking the position, Ridenour was being harassed for trying to do his job of overseeing the security contractor at Rocky Flats. In a letter to then-Energy Secretary Federico Pena, he said "I was instructed by my direct supervisor. . .that my

mission was to 'not negatively impact the contractor' and that I was to 'facilitate the contractor (Kaiser-Hill) winning the award fee'." He resigned several months later, claiming "In my professional life as a military officer, as a Registered Professional Engineer. . .I never before experienced a major conflict between loyalty to my supervision and duty to my country and to the public." (Appendix N)

- Lt. Mark Graf was Alarm Station Supervisor for the Wackenhut protective force at Rocky Flats. Jeff Peters was Director of Protective Force Operations, also at Wackenhut. Both had serious concerns about security at Rocky Flats and wrote to Congressman David Skaggs (D-CO) about these concerns. Peters was placed on administrative leave, his badge and weapon taken from him. He was ordered into counseling. Federal Office of Personnel Management investigators concluded Wackenhut had acted inappropriately and "retaliated" against Peters. In June of 1996, Peters resigned from his position and left Rocky Flats after reaching a settlement agreement with Wackenhut. Lt. Graf's workload was inexplicably raised to 262 hours, from the staff average of 187 hours. After Graf was sent by Wackenhut for psychiatric review, a psychiatrist concluded that Lt. Graf was fit for duty, noting that the reason for Graf's referral was "based on his preoccupation with security safeguards at Rocky Flats and discussion with outside individuals and the media."[20] Lt. Graf was nonetheless fired and finally won a Department of Labor whistleblower case requiring Wackenhut to reinstate him to his original position and pay compensatory damages.

- Edward McCallum was a Colonel in the Special Forces with service in Vietnam. He worked in DOE security for twenty years, and authored the 1996 DOE Annual Report to the President on the Status of Safeguards and Security, which was highly critical of security and caused a serious eruption at DOE. He was immediately put on administrative leave and investigated. In early 1999, McCallum's concerns about the lack of security at Rocky Flats were made public. At about the same time, Secretary Richardson issued a zero-tolerance order against whistleblower retaliation – "Management must also create and foster a work environment that allows free and open expression of security concerns, where workers fear no reprisals or retaliation." (Appendix JJ) It didn't work. McCallum was put on administrative leave based on a security violation accusation that was later dropped. Representative Curt Weldon (R-PA) wrote to his colleagues,

> "Throughout the past decade, this former Green Beret officer attempted numerous times to alert the Administration to grievous lapses in security which left our nation's nuclear facilities vulnerable to foreign espionage and terrorist attack. Officials at the highest levels, including three Secretaries of Energy and White House personnel, consistently ignored Lt. Col. McCallum's warnings, placing our national security in jeopardy. . .Lt. Col. McCallum deserves accolades for what he did to protect our

[20] www.whistleblower.org/www/graf.htm – Downloaded September 14, 2001.

> national security – not the continued destruction of his reputation and career." (Appendix FF)

McCallum took a job at the Pentagon, and is no longer working on security issues at DOE.

- Ron Timm, and his corporation RETA Security, were experienced security analysts under contract to the DOE Headquarters Office of Safeguards and Security. RETA Security was the principal analyst for review of all SSSPs for DOE Headquarters since 1997. He told the IG that he had suffered retaliation for raising concerns about public health and safety. Timm's work assignments analyzing SSSP's for all DOE facilities over the previous five years had plummeted. The IG found no retaliation, as Timm's company was performing other DOE work for Secretary Richardson. As soon as the IG inquiry concluded, Timm's contract was terminated. Timm sent a second letter to the new DOE Secretary, Spencer Abraham, in January 2001 thinking the new administration would look into the ongoing security failures at nuclear facilities. Timm wrote, ". . . time has shown that the existing bureaucracy at DOE have not adequately acted upon the issue of risk to the public other than in ineffective and reactive ways." However, Secretary Abraham delegated the response to the letter to one of the office which Timm accused of covering up security problems, the Office of Independent Oversight. In the six page response Director Glenn Podonsky concluded, "The Department's protection program may not be perfect, we firmly believe it to be effective." Timm is no longer working on Headquarters security issues at DOE and has filed a whistleblower complaint. (Appendix KK; Appendix LL)

- According to an IG Report:

> "one support services contractor believed that an OSS [Office of Safeguards and Security] program manager threatened him with a reduction in contract activity for his role in supporting the SSSP QA [quality assurance] process and for assisting the [Secretary Richardson's] special assistant. The contractor said that he did not receive any contract work in the area of field assistance after the alleged threat was made, and that he viewed the elimination of his field assistance activities as retaliation." (Appendix MM)

The IG concluded that because he did not seek to file a formal whistleblower retaliation complaint and that he continued to receive contracts from the DOE security czar, he had not suffered retaliation. As soon as DOE security czar General Habiger left however, he lost all DOE Headquarters contracts. (Appendix MM)

- In a desperate attempt to shed light on inadequate physical security at the DOE National Labs, a DOE employee faxed two unclassified IG reports that exposed security failures at

DOE to *USA Today* and the *Washington Post*. (These IG Reports are included at the end of this report as Appendices U and MM) As a result, the employee's security clearance was "suspended due to his admitted release, without prior authorization, of a draft DOE Inspector General report on sensitive DOE security matters. His action was in direct contravention of his signed 'Security Responsibility Statement' promulgated by the DOE Office of Security Affairs specifically to prevent such releases," – an illegal internal DOE gag order prohibiting direct contact with the news media. (Appendix KK) According to the Office of Safeguards and Security Notification Letter, the employee "thought that if [he/she] brought this [security] inadequacy to light, then senior DOE officials might be 'sparked' into improving that program. Accordingly, [he/she] decided to send a copy of the draft OIG report to the news media to 'make things better'." That whistleblower is no longer working on security issues for DOE. (Appendix NN)

As Admiral Rickover once warned, "You can sin against God, and God will forgive you – if you sin against the bureaucracy, they will never forgive you!" This old adage certainly describes the culture at DOE.

Budget

"[T]he annual report I wrote. . . said that we were about $150 million dollars underfunded, we've lost 42% of our protective forces and 50% of our SWAT capability. I said that at a time when we've increased our SNM holdings by 70 metric tons. It doesn't take a brain surgeon to figure this one out."

Edward McCallum, Director of Safeguards and Security, DOE (Appendix O)

The security budget competes with the far more politically popular issues in the weapons programs such as stockpile stewardship and weapons research, that command far more Congressional interest. As a result, security ends up as a poor stepchild. For example, during the battle over relocating TA-18 at Los Alamos, the Acting Deputy Administrator for Defense Programs (the predecessor to NNSA) General Thomas Gioconda stated, "Defense Programs' limited capital funding is already allocated to higher priority Stockpile Stewardship projects." (Appendix V)

The former Director of DOE's Office of Safeguards and Security stated, "since 1992, the number of protective forces at DOE sites nationwide has decreased by almost 40% (from 5,640 to the current number of approximately 3,500), while the inventory of nuclear material has increased by more than 30%." At the same time, the total federal budget devoted to DOE security was cut by one-third. No one argues that the terrorist threat had been reduced, in fact, the intelligence community believes the threat is greater today than during the Cold War. (Appendix OO)

In the mid 1990's the cuts were so deep that several sites including Livermore had to disband their SWAT teams. Livermore then had to depend on the Alameda County Sheriffs Department for a SWAT team. The only problem was it took the Sheriff's SWAT team over an hour to mobilize and deploy a force to Livermore – long after a possible attack had taken place. Livermore found a way to overcome this response time problem. According to whistleblowers, in a 1995 force-on-force, the Army Special Forces adversaries found an Alameda County Sheriff's Department helicopter in the air and their SWAT team near the perimeter fence before the attack had started – was the site cheating? The Sheriff told DOE investigators he had been told by the site that prepositioning his forces was acceptable. He understood the test to be one of capability not of timing. Clearly both are important. In 1998, Livermore decided the situation was untenable, and took an additional two years to reconstitute and train a new SWAT team.

In 1999-2000, Secretary Richardson attempted to split the security budget out of the weapons program budget, putting it under the security czar. This was finally accomplished. However, it only lasted for a matter of months before the Congress put the security budget back under the new semi-autonomous National Nuclear Security Agency.

PROBLEMS/SOLUTIONS

PROBLEM: Nuclear Materials Are Spread Across the Country. Weapons-quantity special nuclear materials are stored at 10 fixed sites. This dispersion is a leftover from the Cold War, when there were many more missions for the various sites. Now, a number of sites have virtually no national security mission, however, they continue to store and try to protect tons of nuclear materials at great cost. DOE can not currently adequately protect this material, and security at each site unnecessarily increases redundancies and costs. However, DOE has resisted consolidation as it would threaten fiefdoms and potentially even lead to the closing down of facilities.

SOLUTION: Close Unneeded Facilities. The Base Realignment and Closure Commission should be empowered to recommend closing the unneeded and redundant DOE sites, as well as those sites that have no national defense mission. Not only do the unnecessary sites cost the taxpayers billions annually, but also present a significant health and safety risk to the nearby communities. There have been a number of studies considering the restructuring of the weapons complex over the past ten years. The Bush Administration is currently considering this path. The following are suggestions for closure and consolidation:

- Shut down Idaho National Engineering Lab and the Argonne National Laboratory – West, as they have little or no national defense mission.
- Shut down Hanford, as it has little or no national defense mission.

- Combine Lawrence Livermore in California and Los Alamos National Labs at Los Alamos, NM – we don't need two redundant bomb design labs. Livermore is now in the middle of a highly populated community, yet large amounts of plutonium are stored there.

- Combine Oak Ridge and Savannah River Facilities as both have significantly reduced missions of producing plutonium and fabricating uranium. Rather than repairing or replacing the decaying infrastructure at both sites, it would be more efficient to combine the two.

SOLUTION: Consolidate Nuclear Materials. Another solution to this problem would be to consolidate nuclear materials to fewer, more easily-protected sites. Not only would this save money, it would reduce the risk to the public. A plan by the DOE to consolidate nuclear materials at two sites that should have been operational by now, has been derailed by the bureaucracy. However, two of the most secure facilities in the world are already available. These two facilities would provide enough storage for the entire DOE weapons complex. One is underground in the middle of Kirtland Air Force Base in New Mexico (Kirtland Underground Munitions Storage Complex), and the other is a brand new (and totally unused) highly secure facility, the Device Assembly Facility, at the Nevada Test Site. For the past decade, DOE has been planning a national storage facility for PU at Savannah River and a storage facility for HEU at Oak Ridge. Both are bogged down in a bureaucratic morass with no end in sight.

SOLUTION: Immobilize Excess Nuclear Materials. There is a facility at Savannah River which could be used to meld excess nuclear materials with a radioactive barrier in glass. Once the materials have been immobilized or "vitrified", they would no longer be attractive to terrorists because it would be virtually impossible to reconstitute the immobilized SNM into weapons grade material.

PROBLEM: Bureaucracy Makes Security Tests Easier Rather than Fixing Problems. Without leadership and accountability, there are few incentives for the DOE bureaucracy to address problems. As a result, DOE portrays facilities as being secure and impervious to terrorists and spies when, in fact, they are not. This is largely achieved by sweeping undesirable messages and test results under the bureaucratic carpet and "dumbing down" the current system to hide embarrassing test failures. Ongoing publicized problems at such sites as Los Alamos and the Transportation Safeguards Division attest to this assertion.

SOLUTION: Improve Effectiveness of Protective Forces. Until disparate sites are consolidated, DOE should increase the size of its protective force and improve weaponry, tactics, and command, control, and communication to defend against both theft and radiological sabotage. One possibility would be to explore the option of moving the responsibility for protection of nuclear weapons quantities of special nuclear material to DOD military personnel. The military personnel should not be used for general site

protection of classified information, personnel, or facilities, but only for the protection of SNM. Another possibility would be to explore whether TSD convoys of special nuclear materials should be supported by military personnel. A 1990 GAO report also suggested exploring the possibility of federalizing the protective forces at the sites similar to the protective force of the Transportation Security Division. In interviews the guards [protective force] themselves told GAO investigators, "a federal force would take security more seriously" and that they would "receive better training." (Appendix PP)

PROBLEM: Independence in Nuclear Security is Lacking. The recently Congressionally-created National Nuclear Security Administration (NNSA) exacerbates the problem by elevating the same people who have managed this debacle over the last three decades. As the Rudman report states, due to the "deeply rooted culture of low regard for and, at times, hostility to security issues. . .a reshuffling of offices and lines of accountability may be a necessary step toward meaningful reform, *but it will almost certainly not be sufficient.*"[21]

SOLUTION: Take Security Management Out of DOE. POGO suggests exploring the option of setting up an independent agency to provide security from outside DOE entirely, and leave the many other duties of managing the nuclear weapons complex to the NNSA.

SOLUTION: Move the Independent Oversight Office Out of DOE. Make oversight of nuclear security independent from those charged with implementing security by making the DOE Office of Independent Oversight an Independent Nuclear Facilities Security Board that is independent of DOE. A model would be the Defense Nuclear Facilities Safety Board. This board would report directly to the Congress and be empowered to assess security in the nuclear complex.

PROBLEM: Computers Containing Nuclear Secrets Remain Vulnerable. It is virtually as easy today for a trusted "insider" to put weapons design information on a tape or disk and walk out the door as it was two years ago. All of our known spies have been insiders with the highest security clearances.

SOLUTION: Convert to Media-less Computing. The only way to stop an "insider" is to stop any media (disks, tapes, laptops, etc.) from coming in or out of priority classified areas. At each workstation, the scientist or engineer would only have a monitor, keyboard, and mouse, while the actual computer is locked in a vault. Access to any media would require a "two-man rule" where two people would have to sign-off on any copies.

PROBLEM: DOE Security Forces Cut by 40%. According to testimony from a high-level DOE official, "Since 1992, the number of Protective Forces at DOE sites nationwide has decreased by almost 40% (from 5,640 to the current number of approximately 3,500) while the inventory of nuclear material has increased by 30%." (Appendix OO) The increase has resulted

[21] http://fas.org/sgp/library/pfiab/ – Downloaded September 13, 2001.

from the dismantling of nuclear weapons and the receipt of nuclear materials from the Former Soviet Union. During the same period the threat of terrorism has increased.

> **SOLUTION: Consider Security Budgetary Needs Independently.** Decouple nuclear security funding from scientific research and the nuclear weapons program. Security funding currently competes with scientific research funding from within the National Nuclear Security Administration nuclear weapons budget. Security is always fighting for the scraps after the more politically appealing and bureaucratically popular scientific research and weapons projects are funded.

APPENDICES

Appendix A: Memo from Peter D. H. Stockton, DOE Special Assistant to: Secretary of Energy Bill Richardson, December 20, 2000.

Appendix B: Memo from Richard J. Levernier, Program Manager Assessment and Integration to: Col. Edward J. McCallum, Director Office of Safeguards and Security, December 12, 1998; and

Memo from Richard J. Levernier, Program Manager Assessment and Integration to: Col. Edward J. McCallum, Director Office of Safeguards and Security, April 19, 1999 – with attachments.

Appendix C: Memo from Richard J. Levernier, Program Manager Assessment and Integration to: James L. Ford, Acting Director Field Operations Division, April 11, 2000 – with attachments.

Appendix D: Memo from Peter D. H. Stockton, DOE Special Assistant to: Secretary of Energy Bill Richardson, October 30, 2000.

Appendix E: Partial transcript of speech by General Eugene Habiger at the 41st Annual Meeting of the Institute of Nuclear Material Management.

Appendix F: "Declassification of United States Total Production of Weapon-Grade Plutonium," DOE Facts, December 7, 1993.

Appendix G: "Design Basis Threat for Department of Energy Programs and Facilities (Unclassified)," U.S. Department of Energy Office of Safeguards and Security, December 1998.

Appendix H: Memo from Joseph S. Mahaley, Director Office of Security Affairs to: Acting Deputy Secretary, February 9, 1999 – with attachments.

Appendix I: Memo from Barbara R. Stone, Director Office of Safeguards and Security Evaluations Office of Independent Oversight and Performance Assurance to: General Eugene E. Habiger, Director Office of Security and Emergency Operations, SO-1, August 30, 1999 – with attachment.

Appendix J: Letter from Timothy P. Cole, President Wackenhut Services Inc. to: Terry Vaeth, Manager U.S. Department of Energy, Rocky Flats, July 16, 1992.

Appendix K: Office of Personnel Management interview with William R. Gillison, General Manager, Wackenhut Services Inc., between March 6, 1996 and April 10, 1996.

Appendix L: Report to the President on the "Status of Safeguards and Security for 1996," Office of Safeguards and Security, Office of Security Affairs, Department of Energy, January 1997.

Appendix M: "Verification Assessment Report of the Rocky Flats Environmental Technology Site Safeguards and Security Plan," Department of Energy Internal Memo July 17, 1998.

Appendix N: Letter from Col. David Ridenour, Director Office of Safeguards and Security to: Ms. Jessie Roberson, Manager, DOE Rocky Flats Office, March 31, 1997; and

Letter from Col. David Ridenour, Director Office of Safeguards and Security to: Secretary of Energy Federico Pena, April 16, 1997.

Appendix O: Excerpts of transcript of telephone conversations between Jeffrey Peters, Operational Security Manager, Wackenhut Services, Inc., and Col. Edward J. McCallum, Director Office of Safeguards and Security, May 7 & 8, 1997 .

Appendix P: Letter from Glenn S. Podonsky, Office of Independent Oversight to: J. Owendoff, Acting Assistant Secretary for Environmental Management, EM-1 & Jessie Roberson, Manager Rocky Flats Field Office, May 14, 1998.

Appendix Q: "Comprehensive Inspection of Rocky Flats Filed [sic] Office and the Rocky Flats Environmental Technology Site (U)," Department of Energy Internal Memo, May 1998.

Appendix R: Testimony of Peter D. H. Stockton, former-DOE Special Assistant, U.S. District Court, Colorado, Civil Action No. 97-WM-2191, U.S., ex rel., Col. David Ridenour et al. v. Kaiser-Hill Company, July 2001. This testimony was witnessed and cleared by a Department of Energy classifier to ensure that no classified information was revealed.

Appendix S: Letter from Representative John D. Dingell, Ranking Member, House Commerce Committee to: former Senator Warren Rudman, President's Foreign Intelligence Advisory Board, March 24, 1999; and

Statement of Representative John D. Dingell at the Joint Hearing of the Commerce Committee Energy and Power Subcommittee & the Science Committee Energy and Environment Subcommittee on Restructuring the Department of Energy, July 13, 1999.

Appendix T:	"Debate Widens Over Most Effective Way to Secure Energy Department's Los Alamos Nuclear Site," John J. Fialka, *Wall Street Journal*, March 15, 2000.
Appendix U:	"Summary Report on Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self-Assessments at Los Alamos National Laboratory," U.S. Department of Energy Office of Inspector General, May 2000.
Appendix V:	Memo from General Thomas F. Gioconda, Acting Deputy Administrator for Defense Programs to: the Secretary of Energy Bill Richardson, March 2000.
Appendix W:	Letter from Ronald E. Timm President, RETA Security to: General Eugene Habiger Director, Office of Security & Emergency operations, SO-1, January 5, 2000.
Appendix X:	Letter from Maureen McCarthy and Ellen Livingston to: Secretary of Energy Bill Richardson, November 21, 2000.
Appendix Y:	Letter from General John A. Gordon, Administrator National Nuclear Security Administration to: Dr. John Browne, Director Los Alamos National Lab November 22, 2000.
Appendix Z:	"Weaponry: Availability of Military .50 Caliber Ammunition," General Accounting Office Report # OSI-99-14R, June 30, 1999.
Appendix AA:	"Improvised Explosive Devices (IEDs) and Other Criminal and Terrorist Devices: A Basic Reference Manual," Director of Central Intelligence, Interagency Intelligence Committee on Terrorism, September 2000.
Appendix BB:	"DOE Probes New Security Lapse And Accident at Los Alamos Lab," John J. Fialka, *Wall Street Journal*, December 11, 2000.
Appendix CC:	Overheads from Integrated Cyber Security Initiative, August 29 & 30, 2000.
Appendix DD:	Letter from Peter D. H. Stockton, former DOE Special Assistant to: Senator Richard Shelby, September 13, 2001.
Appendix EE:	"Draft Statement of Facts, Nuclear Security: Improvements Needed in DOE's Safeguards and Security Oversight," General Accounting Office Draft Report, December 14, 1999.
Appendix FF:	Dear Colleague letter from Representative Curt Weldon, June 22, 1999.
Appendix GG:	"Memorandum for the Headquarters NNSA Team," Bob Kuckuck, Principle Deputy Administrator, National Nuclear Security Administration, August 20, 2001.

Appendix HH: Energy Appropriations FY2002 House of Representatives Report.

Appendix II: "Department of Energy: Key Factors Underlying Security Problems at DOE Facilities," General Accounting Office Testimony #T-RCED-99-159, April 20, 1999.

Appendix JJ: "Memorandum for All Department and Contract Employees," Secretary of Energy Bill Richardson, June 17, 1999.

Appendix KK: Letter from Glenn S. Podonsky, Director of Office of Independent Oversight to: Ronald E. Timm, President RETA Security, March 5, 2001.

Appendix LL: Letter from Ronald E. Timm, President RETA Security to: Secretary of Energy Spencer Abraham, February 9, 2001.

Appendix MM: "Summary Report on Allegations Concerning the Department of Energy Site Safeguards and Security Planning Process," Department of Energy Office of Inspector General, September 2000.

Appendix NN: DOE Notification Letter from Owen Johnson, Director Office of Safeguard and Security, October 26, 2000.

Appendix OO: Statement of Col. Edward J. McCallum, Director Office of Safeguards and Security, June 8, 1999.

Appendix PP: "Nuclear Safety: Potential Security Weaknesses at Los Alamos and Other DOE Facilities," General Accounting Office Report #RCED-91-12, October 1990.

Acronym Glossary

DIA - Defense Intelligence Agency

DBT - Design Basis Threat

EIS - Environmental Impact Statement

GAO - General Accounting Office

HEU - Highly Enriched Uranium

IND - Improvised Nuclear Device

IG - Inspector General

JTS - Joint Tactical Simulations

LANL - Los Alamos National Lab

MILES - Multiple Integrated Laser Engagement System

M&O - Management and Operations

NNSA - National Nuclear Security Administration

OIG - Office of Inspector General

OSS - Office of Safeguards and Security

OSSE - Office of Safeguards and Security Evaluations of the Office of Independent Oversight and Performance Assurance

PDD - Presidential Decision Directive

PF - Protective Force

PU - Plutonium

QA - Quality Assurance

SAP - Special Access Program

SNM - Special Nuclear Materials

SSSP - Site Safeguards and Security Plan

TA - Technical Area

TSD - Transportation Security Division

VA - Vulnerability Analysis

WMD - Weapons of Mass Destruction

Ms. BRIAN. We concluded that the Nation's 10 nuclear weapons facilities, which house nearly 1,000 tons of weapons-grade plutonium and highly enriched uranium, regularly fail to protect this material during mock terrorist attacks. Many of these sites are located near metropolitan areas, including the San Francisco Bay area, Denver, Albuquerque and Knoxville.

There are three major threats to these facilities, and only two were really discussed in the previous testimony—theft, radiological sabotage, or a dirty bomb, and as Mr. Shays has made reference to, the possibility of terrorists creating an improvised nuclear device, a sizable nuclear detonation within minutes.

In full-scope mock terror attack tests performed by the government at DOE facilities, half the time mock terrorists are successful in breaking in, stealing significant quantities of special nuclear material and leaving the site. Theft, however, requires that the terrorists get into the facility and back out with the material. A suicidal terrorist would not have to work that hard. Instead, a successful suicidal terrorist attack doesn't require getting out again and could create a dirty bomb or a sizable nuclear detonation at the facility itself.

For example, in October 2000, there was a mock attack test of security at technical area 18, a facility at Los Alamos. The mock terrorists successfully entered the facility and the guard force could not get them out. The mock terrorists had enough time to have been able to create a sizable nuclear detonation. A recent CIA pamphlet summarizing devices of interest to al Qaeda and other terrorist groups highlighted both dirty bombs and improvised nuclear devices as two of their greatest concerns.

We believe the single most important element to improve security at the nuclear weapons facilities is a realistic design basis threat. Twenty months after September 11, DOE finally substantially increased the design basis threat at level 1 sites. Unfortunately, the upgrades will not be fully implemented until 2009, which is 8 years after September 11.

The other nuclear weapons sites, however, still have a long way to go, and the new design basis threat for them is wholly inadequate. Special operations personnel expect the terrorist attack on one of these facilities to be with a squad-sized unit. The Army Special Forces sizes a squad at 12 people and the Navy SEALS size a squad at 14 attackers. The way we understand it, even under the new design basis threat for these level 2 facilities, which have improvised nuclear device vulnerabilities, DOE will only be protecting against far fewer attackers.

Currently, DOE is determining its security requirements based on how much money it is willing to spend on security, and this is backward. Now, I heard Ambassador Brooks saying that wasn't true, but I would bring your attention to the testimony of the GAO on page 14, where they said, "The DOE and NNSA officials from all levels told us that concern over resources played a large role in developing the 2003 DBT, with some officials calling the DBT the 'funding basis threat,' or the maximum threat the Department could afford. This tension between threat size and resources is not a new development." Hopefully, the committee can encourage DOE

to determine its security needs based on the Intelligence Community's postulated threat in your closed session.

We keep seeing evidence of security failures even without an attack on these facilities. All three of the weapons labs have had serious management and security problems in just the last few months. Again, Ambassador Brooks suggested these were not security problems. But let me describe some of them.

Top security officials at both Los Alamos and Livermore have been replaced. Only 6 months ago what began as a management scandal involved security issues including over 300 stolen or missing computers that the IG testified before Congress may have contained classified information. Now we have missing plutonium there.

At Livermore, a set of keys and a security card to access-sensitive areas were missing for weeks without being reported. And that is not a security problem?

In addition, members of the Livermore SWAT team claimed they could not defend the lab in the event of a terrorist attack. At Sandia, there has also been a series of security lapses, including guards sleeping and keys missing that are being investigated by Senator Grassley. These scandals, I'd like to point out, have never been discovered by DOE; they've only been brought forward by outsiders.

And with reference to there not being retaliation, when you're talking about these particular instances, you can look at the Los Alamos investigators, who were fired after their findings were revealed internally, not to the press, as an example of retaliation that does happen.

The scattering of special nuclear materials across the country is left over from the cold war.

Now, a number of sites have virtually no national security mission; however, they continue to store and try to protect tons of nuclear material at great cost. However, DOE has resisted many consolidation opportunities, as it would threaten fiefdoms and potentially even lead to the closing down of facilities.

In addition to requiring the design basis threat that will address improvised nuclear device vulnerabilities, POGO makes the following recommendations.

Consolidation of nuclear materials: The Base Realignment and Closure Commission should be empowered to recommend closing the unneeded and redundant DOE sites, as well as those sites that have no national defense mission. Another solution would be to consolidate nuclear materials to fewer, more easily protected sites. These solutions save money and reduce the risk to the public.

Under Secretary Robert Card himself recently advised that the first question for a site to consider is "Is there a way to reduce the targets by consolidating material or, even better, exporting material to other more permanent or hardened sites?" And I have the letter if you need that. This is certainly commendable language. However, these same directions have been issued to the field for more than 20 years with little or no impact.

A case in point, again, is Los Alamos' technical area 18. In 2000, Secretary Richardson directed the site to be deinventoried of its special nuclear materials by 2003. It was to be moved underground

to a currently empty and hardened underground facility at the Nevada Test Site. Here we are and not one gram has moved in that direction.

Ambassador Brooks's recent predecessor has also pushed to expedite moving the materials out of TA 18, apparently to no avail. I believe Los Alamos is betting on turnover at DOE headquarters and the inattention of the Congress.

I would also like to challenge earlier testimony that the security tests are no longer seriously dumbed down. I have examples from last month. Last month, during a mock theft scenario, terrorists were not allowed to go out the same hole in the fence they came in, requiring them to run all the way around the fence line to leave the facility. If they had been allowed to use the hole, they would have been able to leave the facility without even having engaged any of the protective forces.

In another recent example, the mock terrorists were required to stay on the road in order to leave the facility.

In addition, as was pointed out, advance warning is given to sites, often months in advance, that a test is scheduled and the test, as we've mentioned, follows scripts of what the terrorists can and can't do.

The three advantages a terrorist has are surprise, speed and violence of action, elements that are not factors in these dumbed-down tests. Yet the mock terrorists still accomplish their mission all too often.

Immobilized excess plutonium: Over 50 tons of our plutonium have already been declared excess and could be immobilized, making it less attractive for theft.

One way to counter DOE's antisecurity culture is to move security oversight out of DOE. One suggestion is to move the independent oversight office to model something like the Defense Nuclear Safety Facility Board where he's not having to report directly to the Secretary. Another option would be to make security oversight at DOE facilities a DOD responsibility, perhaps under the Nuclear Command and Control staff.

Increase security funding, but spend resources more efficiently: The United States spends over $1 billion annually on security at DOE sites. We are not getting our money's worth. We are spreading our resources inefficiently by protecting sites we should not have to protect, either because special nuclear materials are not needed there or it's not needed there in massive quantities. Clearly, the new DBT will require more money, but money should not be thrown at the problem without evidence that a real plan to implement security upgrades efficiently is in place.

I'd like to point out that, in the past, DOE security has hit obstacles obtaining increased budgets from within the Department, OMB and from Congress, in large part because they've simply lied about the status of security.

For example, in early 2002, then-NNSA Administrator Gordon wrote a letter to the Washington Post denying POGO's findings and assuring the public that security was adequate at the nuclear sites. One month later DOE was talking out of the other side of their mouth, begging OMB and the Congress for a half-billion dollar increase in funding because of dire security problems.

Finally, more congressional oversight: Without sustained and intensive scrutiny and oversight, DOE briefings and testimony will not reveal the actual status of security. It is ultimately up to Congress to keep at this, and I believe it is some of the most important work that you'll do.

Here's a suggestion for a next step: In mid-2002, the Scowcroft Commission finally issued their end-to-end review of security at DOD and DOE nuclear weapons facilities. We encourage the committee to obtain copies of the draft of that report and interview the authors.

If I could—because I am not going to be in the closed session, if I could just make two more——

Mr. TURNER. Your time is running out, so if you could conclude quickly.

Ms. BRIAN. Yes, I just wanted to say we already know what's wrong.

Ambassador Brooks had said we need more review, but the last administration, for example, created the position of security czar headed by an Air Force general with no obvious improvement. I would humbly suggest that roles and responsibilities are periodically rearranged, but we still aren't protecting our nuclear materials against the real terrorist threat; and it is going to take serious congressional oversight to make sure it happens.

Thank you for your inviting me to testify.

Mr. TURNER. Thank you.

[The prepared statement of Ms. Brian follows:]

Testimony of
Danielle Brian, Executive Director
Project On Government Oversight
on
Inadequate Security at the Department of Energy Nuclear Weapons Complex
before the
House Government Reform Subcommittee on National Security,
Emerging Threats and International Relations
June 24, 2003

Mr. Chairman, I commend you for holding these important hearings. The Project On Government Oversight (POGO) is an investigative organization that works with inside sources to improve public policy. Founded in 1981, POGO is a politically-independent, nonprofit watchdog that strives to promote a government that is accountable to the citizenry.

In early 2001, POGO began its investigation into nuclear security at the Department Of Energy (DOE) after more than a dozen high-level departmental security experts came forward with concerns regarding inadequate security at the DOE's nuclear weapons facilities. Just prior to September 11, 2001, POGO completed that investigation, concluding that the nation's ten nuclear weapons facilities, which house nearly 1,000 tons of weapons-grade plutonium and highly-enriched uranium, and the transportation system for weapons and nuclear materials regularly fail to protect this material during mock terrorist attacks. The results of that investigation were issued in the POGO report, "U. S. Nuclear Weapons Complex: Security at Risk." Even though it is now two years old, I daresay the problems identified are still relevant today. I ask that it be included in the record.

We briefed the NSC on multiple occasions, Homeland Security, various Pentagon groups including the Scowcroft End-to-End Review team, the Nuclear Command and Control staff, the White House OMB, among others, on our findings. We were encouraged when we met with officials of Homeland Security, who had seemed to understand the problems at DOE. They were particularly aware of problems with DOE oversight of the facilities, specifically personnel who continue to defend the status quo. In fact after our briefing to Homeland Security, I expected them to look at me with disbelief. Instead, however, a detailee from the Pentagon said, " You realize we are more concerned about the lack of security at DOE facilities than you are." They advised that they were establishing red teams to independently test security at DOE facilities in the April 2002 time frame. However, it never happened.

There are ten major DOE sites that have weapons quantities of plutonium and highly-enriched uranium, many of which are located near metropolitan areas including the San Francisco Bay area, Denver, Albuquerque and Knoxville. In order to perform their missions, a number of these sites do not need any Special Nuclear Material, and others certainly don't require the quantities that are currently being stored at the sites, but bureaucratic fiefdoms protect the status quo. There are three major threats to these facilities:

- theft of plutonium or highly-enriched uranium to create a crude nuclear weapon;
- terrorists gaining access to plutonium and highly-enriched uranium and using conventional explosives to create radiological sabotage, or a dirty bomb; and
- terrorists gaining access to plutonium and highly-enriched uranium and creating an Improvised Nuclear Device (IND) – a sizable nuclear detonation within minutes.

Weapons grade material stolen from a DOE facility could be used by a terrorist group to either fabricate a crude nuclear weapon or create a "dirty bomb." This is not as far-fetched as some might believe. In fact, in full-scope mock terrorist attack tests performed by the government at DOE facilities, half the time mock terrorists are successful in breaking in, stealing significant quantities of Special Nuclear Material and leaving the site.

Theft, however, requires that the terrorists get into a facility and back out with the material. What we have found in our investigations is that a suicidal terrorist would not have to work that hard. Instead, a successful suicidal terrorist attack at several of our DOE weapons facilities could result in a sizeable nuclear detonation at the facility itself. A terrorist group does not have to steal nuclear material, create a nuclear device, transport it to the United States, and detonate it in a major city. They could simply gain access to the material at a U.S. nuclear facility - some of which are near large metropolitan areas - and tests have shown they could accomplish the same outcome. This type of homemade bomb is called an Improvised Nuclear Device, or IND. Such a detonation can be created by using conventional explosives brought into the facility in a backpack and combined with particular kinds of Special Nuclear Materials stored at these sites.

For example, in October 2000, there was a mock attack test of the security at Technical Area-18, a facility at Los Alamos National Laboratory that contains many tons of Special Nuclear Material. The mock terrorists successfully entered a facility and the guard force could not get them out. The mock terrorists had enough time to have been able to create a sizeable nuclear detonation. The Senate Foreign Relations Committee held important hearings on this threat in March of 2003. In fact, in a recent CIA pamphlet summarizing typical Chemical Biological Radiological and Nuclear devices of interest to al-Qaida and other terrorist groups, they highlighted both dirty bombs and Improvised Nuclear Devices as two of their greatest concerns.

Improvised Nuclear Devices pose a great concern at a number of DOE facilities. In the mid-90s, the DOE made this vulnerability a highly-classified "Special Access Program"(SAP), and as a result no one could even talk about it unless you were one of the select few with a "need to know" – even though the problem is simple physics. Many inside DOE believe it was "SAPPED" because they didn't want to spend the money to address the vulnerability. A few months after a discussion of this vulnerability in the POGO report based on unclassified sources, General John Gordon, then-National Nuclear Security Administration (NNSA)Administrator, ordered a major change in security strategy to address the Improvised Nuclear Device vulnerability. Until that time, the strategy at most sites with Improvised Nuclear Device vulnerabilities was to "contain" the terrorists in the facility, and not let them out. Guards now are supposed to "deny" terrorist access to the facilities, because if the terrorists do get access to certain kinds of material, they can create an Improvised Nuclear Device in minutes. This is a very important step, if DOE can actually implement it.

We believe the single most important element to improve security at the nuclear weapons facilities is a realistic Design Basis Threat (DBT). The DBT is the threat that these facilities are required to defend against – the number of outside attackers with the help of active and passive insiders. It also includes the kinds of weapons likely to be used by potential adversaries. In May 2003, 20 months after 9/11, DOE finally substantially increased the DBT at Level 1 sites– sites with full-up nuclear weapons, test devices and partially dismantled or assembled weapons. DOE deserves credit for this important step, unfortunately the upgrades will not be fully implemented until 2009– eight years after 9/11.

The other nuclear weapons sites, however, still have a long way to go and the new DBT for them is wholly inadequate. POGO has learned from Special Operations personnel and others in the Pentagon that al-Qaida would be expected to attack one of these facilities with a squad sized unit – The Army Special Forces size a squad at 12, and the Navy SEALS size a squad at 14 attackers. The way we understand it, even under the new DBT for Level 2 facilities – which contain large quantities of weapons grade plutonium and uranium with Improvised Nuclear Device vulnerabilities – DOE will only be protecting against far fewer attackers. Currently, DOE is determining its security requirements based on how much money it is willing to spend on security. This is backwards. Instead, DOE should determine the realistic threat, then require the facilities to size the protective strategy to meet that threat. Hopefully the Committee can encourage DOE to determine its security needs based on the intelligence community's Postulated Threat in your closed session.

We keep seeing evidence of security failures even without an attack on these facilities. All three of the weapons labs have had serious management and security problems in just the last few months. Top security officials at both Los Alamos and Livermore have been replaced. Only six months ago, a management scandal broke, involving some security issues including over 300 stolen or missing computers that the IG testified before Congress may have contained classified information. Now we have missing plutonium. At Livermore a set of keys and a security card to access sensitive areas were missing for weeks without being reported. In addition, members of the Livermore SWAT team claim they could not defend the lab in the event of a terrorist attack. At Sandia, there has also been a series of security lapses including guards sleeping and keys missing that are being investigated by Senator Grassley. Clearly security still takes a back seat at these facilities.

The scattering of special nuclear materials across the country is a leftover from the Cold War, when there were many more missions for the various sites. Now, a number of sites have virtually no national security mission, however, they continue to store and try to protect tons of nuclear materials at great cost. Currently, DOE cannot adequately protect this material, and security at each site unnecessarily increases redundancies and costs. However, DOE has resisted many consolidation opportunities as it would threaten fiefdoms and potentially even lead to (gasp) the closing down of facilities.

In addition to requiring a DBT that will address Improvised Nuclear Device vulnerabilities, POGO makes the following recommendations:

CONSOLIDATION OF NUCLEAR MATERIALS

The Base Realignment and Closure Commission should be empowered to recommend closing the unneeded and redundant DOE sites, as well as those sites that have no national defense mission. Not only do the unnecessary sites cost the taxpayers billions annually, but also present a significant health and safety risk to the nearby communities.

Another solution to this problem would be to consolidate nuclear materials to fewer, more easily-protected, sites. Not only would this save money, it would reduce the risk to the public. A plan by the DOE to consolidate nuclear materials at Savannah River and Oak Ridge at underground facilities should have been operational by now, but has been derailed by the bureaucracy. On May 28, 2003 Undersecretary Robert Card, in a Memorandum to the Program Offices, advised that,

> "The first question for a site to consider is 'is there a way to reduce the targets by consolidating material, documents, vaults, and access areas or even better, exporting material or documents to other more permanent or hardened sites?' Target reduction is preferred to adding personnel or technology to protect current targets, and it better responds to the possibility of further DBT increases."

This is certainly commendable language, however, these same directions have been issued to the field for twenty years with little or no impact. In recent years, there has been some marginal consolidation within sites. Some small DOE sites with little or no Special Nuclear Materials have been shut down. Rocky Flats is the only site with significant quantities of plutonium that is in the process of being de-inventoried. However, there has been no effort to move this material to underground sites which can be more economically and effectively protected.

A case in point is TA-18 at Los Alamos. In 2000, then-Energy Secretary Bill Richardson directed that this site, which is at the bottom of a canyon and cannot be protected, be deinventoried of its Special Nuclear Materials by 2003. These materials and the mission were to be moved underground to a currently empty and hardened underground facility at the Nevada Test Site. Here we are, and not one gram has moved in that direction. Last year, NNSA Deputy Administrator Everet Beckner ordered then-Lab Director John Browne to expedite the deinventorying. New excuses are emanating from Los Alamos that they still aren't ready, but will begin moving the materials in 2006. I believe they are betting on turnover at DOE Headquarters, and the inattention of the Congress.

MAKE TESTS MORE REALISTIC

According to experts interviewed by POGO, including former and current members of Special Forces units used to test security at sensitive facilities, and current and former DOE and DOD officials, the tests of security at the weapons facilities are still seriously dumbed-down – often to the point of absurdity. For example, just recently during a mock theft scenario, "terrorists" were not allowed to go out the same hole in the fence they came in, requiring them to run all the way around the fence line to leave the facility. If they had been allowed to use the hole, they would have

been able to leave the facility without even having engaged any of the protective forces. In another recent example, the mock terrorists were required to stay on the road in order to leave the facility. DOE should use trained adversary forces, for example the Special Forces unit out of Fort Bragg, or the Navy SEALs to perform these tests. These teams are trained to think and act like terrorists. Instead, typically protective forces from other sites are used as mock terrorists – yet they lack this very specialized training. In addition, advanced warning is given to the sites – often months in advance – that a test is scheduled, and the tests follow scripts of what the "terrorists" can and can't do. The three advantages a terrorist has are surprise, speed and violence of action – elements that are not factors in these dumbed-down tests – yet the mock terrorists still accomplish their "mission" all too often.

IMMOBILIZE EXCESS PLUTONIUM

Over 50 tons of our plutonium have already been declared excess and could be immobilized - glassified and surrounded with a radiation shield so that it would be less attractive for theft. Instead of moving ahead with this plan, however, the U.S. has decided to bet on an unproven technology of turning this excess plutonium into reactor fuel called MOX, which will still result in the creation of more plutonium. We believe this is a mistake. Until the excess plutonium is permanently immobilized, it will continue to pose an unnecessary homeland security vulnerability.

MOVE SECURITY OVERSIGHT OUT OF DOE

The Congressionally-created National Nuclear Security Administration (NNSA) exacerbated the problem by elevating the same people who have managed this debacle over the last three decades, and the culture has not changed. All the way up the chain of command, from the contractor self-assessments, the Area Offices, Operations Offices have been found by the IG and GAO to have been all too willing to sugar-coat, and sometimes even falsify their security reports.

One way to counter this culture is to improve oversight of security, and move the Independent Oversight Office out of DOE. Oversight of nuclear security should be more independent from those charged with implementing security by making the DOE Office of Independent Oversight an Independent Nuclear Facilities Security Board that is separate from DOE. A model would be the Defense Nuclear Facilities Safety Board. This board would report directly to the Congress and be empowered to assess security in the nuclear complex.

Another option would be to make security oversight of DOE facilities a DOD responsibility, perhaps under the Nuclear Command and Control Staff. Given that the materials stored at DOE facilities are often equally attractive to terrorists as those stored at DOD sites, and DOD is the "customer" for DOE made weapons, it is perfectly appropriate to have our most highly trained security specialists responsible for this job.

INCREASE SECURITY FUNDING, BUT SPEND RESOURCES MORE EFFICIENTLY

The United States spends over $1 billion annually on security at DOE sites. We are not getting our money's worth. We are spreading our resources inefficiently by protecting sites we should not have to protect either because Special Nuclear Materials are not needed there, or it is not needed there in massive quantities. Clearly the new DBT will require more money, but money should not be thrown at the problem without evidence that a real plan to implement security upgrades efficiently is in place. The first step is to consolidate and store the materials underground. In the past, DOE security has hit obstacles obtaining increased budgets from within the department, from OMB and from the Congress in large part because they have simply lied about the status of security. For example in early 2002, then-NNSA Administrator Gordon wrote a letter to the Washington Post denying POGO's findings, and assuring the public that security was adequate at the nuclear sites. One month later, DOE was talking out of the other side of its mouth begging OMB and the Congress for a half-billion dollar increase in funding because of dire security problems.

MORE CONGRESSIONAL OVERSIGHT

There are two things that move any bureaucracy: one is sustained press attention to a problem and second is congressional oversight. Over the last 20-30 years, there has never been sustained press attention paid to security debacles at DOE because the Department has been able to hide behind overclassification.

According to the President's Foreign Intelligence Advisory Board, "The panel has found that DOE and the weapons laboratories have a deeply rooted culture of low regard for and, at times, hostility to security issues, which has continually frustrated the efforts of its internal and external critics, notably the GAO and House Energy and Commerce Committee." POGO compiled a list of over 50 reports, hearings, testimony, Commissions detailing DOE security failures – not including the more recent IG and GAO findings.

The Congressional hearings spurred by the Los Alamos cyber security breaches focused on two specific incidents of security failures, Wen Ho Lee and the missing hard drives, but did not deal with the systemic physical and cyber security problems at the nuclear weapons complex. Incidentally, no significant security improvements have been implemented as a result of these high profile cases. Without sustained and intensive scrutiny and oversight, DOE briefings and testimony will not reveal the actual status of security. It is ultimately up to Congress to keep at this. I believe it is some of the most important work you can do.

Here's a suggestion for a next step: In mid-2002 the Scowcroft Commission finally issued their "End-to-End" review of security at DOD and DOE nuclear weapons facilities. We were advised that drafts of that report were very critical of DOE security and oversight. Despite Rep. Markey's request to see a declassified version of the report, it was never released. Apparently the GAO never saw the drafts or the final version of that report either. We encourage the Committee to obtain a copy of the drafts of the report and interview the authors.

Thank you very much for commissioning this GAO report and inviting me to testify.

Mr. TURNER. Mr. Timm.

Mr. TIMM. Thank you. Good morning Mr. Chairman. I would like to thank you and the subcommittee for inviting me to give my professional opinion on the state of security at the nuclear weapons facilities in the Department of Energy. I look forward to presenting you to a national security problem that only Congress can solve and that has potential consequences equivalent to that of September 11.

I prepared some slides since we were in a different room before, but you can read along with those, which may be of help when I go through mine, because there are technical things I'll refer to.

According to the committee's letter of invitation sent to me, you said the purpose of the hearing was to determine the adequacy of security in the Department of Energy. In fact, this morning a couple of times you've asked the question about adequate security.

The expression "adequate" is a layperson's term. The Department has very prescriptive definitions of risk, or the consequence of loss of nuclear materials and risk to the health and safety of the public. Risk in a vulnerability analysis report is developed as a quantitative value that has, in turn, provided adjectival designations of high, moderate or low. When a site is determined to be at high risk, compensatory measures must be implemented by orders within 24 hours. A simple red flag we should look for in a description of risk is "adequate" which is in fact an obfuscation of the risk state.

Based on past Department of Energy policy and management and my current activities in the Department, I fear that we remain at high risk today. I urge to you look into this critical concern. I further urge you not to accept the canned response of "we fixed it" without clear verification. In fact, I heard a typical of that this morning by saying they had 18-month-old data. People who long tolerated and even abetted the failings in the Department are still there, with no one else to oversee their action.

You have asked what have the assessments shown. The assessment, particularly the headquarters quality assurance team's efforts, documented high risk at certain sites. For example, from 1997 to 2000, I was principal author of over 200 classified and unclassified letters and reports prepared by the quality assurance team that identified high risk to three major DOE facilities with tons of highly enriched uranium and plutonium holdings. And if you'd look at slide 2, you will see that QA group was made up of headquarters personnel. It was made up of senior personnel from my company, the Sandia National Laboratory simulation personnel and the Army Special Forces testing people that do force-on-force testing. All together there were something like 20 people involved with that.

The assessments included the theft of special nuclear materials and sabotage resulting in either an improvised nuclear device or a radiological dispersal device.

At that time, I personally briefed the findings of high risk to Department of Energy Directors Joe Mahaley and Toby Johnson. Neither one acted in accordance with Department of Energy orders. Some of these same issues were briefed to Secretary Richardson,

and they were staffed down to the same two persons and nothing was done to address the vulnerabilities.

Members of the quality assurance team surmised that what happened in these instances was that OSS, now the Office of Security, voted the issues to the two responsible program offices, Defense Programs and Environmental Management, where there was immediate reluctance to address the issue. There was continuous foot-dragging by each of these programs' offices in regards to evaluating the consequences of loss of nuclear materials or the definitions and characteristics of a design basis threat.

For example, when developing a worse case scenario, the quality assurance team would often assume to arm the terrorists with 50-caliber sniper rifles with armor-piercing incendiary rounds. The program offices argued that this was unfair to the protective forces. Regularly, the program officer would balk at the high-risk determination at a site because if they were to acknowledge the state of risk, they would have to fix it while immediately instituting compensatory measures that would divert funds from programmatic efforts.

To paraphrase a recent quote from Steve Wallace at the Columbia Accident Investigation Board, what seems to have evolved is that higher-level decisionmakers came to the conclusion that there isn't a security issue, in part based on analysis done by analysts who sort of wanted low risk.

How is risk assessed? And this where you are not going to want to follow me a lot because you have seen an equation on that one. But, basically, risk is assessed by a simple equation called R = C x T x (1—PE), and the term "consequence" is the value of the consequence of loss of theft or sabotage of nuclear materials and danger to the health and safety of the public.

The "T" value is, in fact, the design basis threat and describes what all the attributes and characteristics of the terrorists are.

"PE" is a value that basically is the protection elements that you're talking about on a site. It's made up of protection delay and response.

And if you look at that, there are some funny arrows on it. If you remember from your days back in algebra, when one side of the equation goes up, the other side of the equation has to go up in order to remain balanced—with the exception that "1—PE," in order to get better protection to reduce risk, you have to get better protection coming up. And that's what we're here talking about, protection adequate to keep the risk low in the Department.

In and of itself, the equation for risk is algebraically perhaps deceptively so. For example, in physics the equations developed by Newton and Einstein, F = ma and E = mc2 are also simple. However, one determines space flight and one develops nuclear weapons. The risk equation in the Department of Energy is used in terms of the protection required for the assets of societal importance, that is, the theft or sabotage of nuclear materials from national inventory under the stewardship of the Department of Energy.

Nineteen months after the September 11 attack, a new design basis threat was finally issued at the end of May. A draft version had been circulated on December 31 that included an increase in

the number of terrorists and a lowering of the numerical value for risk. The draft design basis statements would have approved one failure in every 20 attacks at the low risk. That means every time they tried 20 times, they would have succeeded once and that was the standard they wanted to move to.

Today's new design basis threat that was approved less than 3 weeks ago has a much higher rate of loss. It is the same rate of loss used before September 11 attacks. On September 11, the terrorists succeeded in three out of four attempts. Either an addition to the number of terrorists or a decrease in the approved low risk would result in a linear increase in the size of protective force for a given site. By making just one change in the design basis threat, the security improvements are simplified. Even with the new and simple changes to the design basis threat, the necessary improvements in security are not required to be completed until 2009, with the actual improvements to be sometimes later.

Sometimes on physical security you will approve the money and it will not be turnkeyed until 3 years later. So the question I was asked before about, are we going to still be talking about this in 2008 and 2010, there's an extremely high likelihood, based upon what we've had in past track records.

I have talked about the risk of nuclear weapons complex and the Department and the risk of health and safety to the public, as well as the corrective actions for approved design basis threat. But how do we fix it? There is no quick fix in the Department that has been dysfunctional as long as this department has, but there are corrective systems to improve process, and they are: You must hold senior managers in the Department accountable for their actions. Many of the current managers in the Department knew and know about high risk and nuclear inventory and theft or sabotage, and they were given thousands of pages of classified reports documenting the high risk. To date, reorganization of the Department to include NNSA has only rearranged the deck chairs. We need to replace these people with qualified personnel.

The bureaucrats in place protect one another. You can't expect friends to fire one another. In this case, only the Congress can effect that change.

Top leaders should be held accountable. Their actions should put their careers on the line. Today, one of the aforementioned Department of Energy Directors has been given an award and the other is at Lawrence Livermore Laboratory looking at a security failure of the lost keys. What we need are qualified personnel with experience in loss prevention, not simply retired military personnel whose experience is in national defense or law enforcement.

In fact, I viewed with some amusement Secretary Brooks saying that I am bringing in "admiral this" and "admiral that." We have had Air Force generals come in. They are national defense experts or they are law enforcement experts; they are not loss prevention experts. And so that in itself—they have—in fact, we have seen them walk out to the site and say they've got big guns at this site. You walk out with a dirt-faced Special Forces guy, and he will show you what a big gun can do to some of those people that are walking around out there.

The second recommendation is to consolidate the nuclear materials, and that was pretty much what Danielle had, and I agree with that. We have seen plans put in place by the previous—to have Decision Directives to move materials. Malicious compliance is being done by the Department that says we still haven't moved it to date.

The other last item that is most important from your perspective is providing the line item funding for physical security at the level of a program office to include the operating dollars designated for increased protective force size and capabilities.

Today, the Department of Homeland Security has a budget greater than $30 billion. However, Department of Energy management resists spending money on security. If they establish a new 24/7 post or patrol for the protective force at any of the 10 Class A sites, this is equal to about five full-time protective force personnel, which is the same cost as two or three scientists. Therefore, the scientists must be laid off to hire the security personnel, not a popular option. The program offices have an inherent conflict of interest when deciding to improve security and lower risk or lay off scientists.

In conclusion, let me summarize my testimony. Many of the nuclear weapon facilities in the Department of Energy are at risk, which endangers the health and safety of the public. This has been documented continuously since March 1997. The security of the Nation's nuclear stockpile has been mischaracterized as adequate by senior career personnel within the Department. The corrections and remedies for the existing problems fall to Congress for action.

Thank you very much.

[The prepared statement of Mr. Timm follows:]

Copyright: RETA Security, Inc. 2003

Testimony of
Ronald E. Timm, Certified Protection Professional
President, RETA Security, Inc.
to the 108th Congress, House of Representatives
Committee of Government Reform
Subcommittee on National Security, Emerging Threats and International Relations
June 24, 2003

Good morning, Mr. Chairman. I would like to thank you and the subcommittee for inviting me to give my professional opinion on the state of security at the nuclear weapon facilities in the Department of Energy. I look forward to presenting to you a serious national security problem that only Congress can solve that has the potential consequence equivalent to 9/11.

For the past 20 years I have been continuously participating in security programs for all of the Class A facilities and transportation of Category I quantities of special nuclear materials in the Department of Energy. I am currently doing more limited work in security at the Department of Energy operations office level that keeps me current in Department of Energy activities. My contracted work consisted of security engineering of detection systems (typically alarms and closed circuit television) and delay systems (typically barriers) and vulnerability analysis of the risk to the nuclear materials from theft or sabotage. After making my concerns about inadequate security to Department of Energy headquarters, and the current administration, my headquarters work was terminated. Today, I am actively involved in homeland security concerns to include such diverse work as the vulnerability analysis for Mount Rushmore and the National Park Service, and engineering for security of dams for the Corps of Engineers.

In 1997 I began an assignment at headquarters to provide quality assurance of the vulnerability analysis for the Safeguards and Security Plans for the 10 Class A Category I special nuclear materials sites and the Transportation Division. The quality assurance effort was initiated by Col. Edward McCallum the Director of the Office of Safeguards and Security Division for Department of Energy. He is now the Director of the Department of Defense's Technical Security Working Group. The quality assurance program was a team effort of 15 to 20 multi-disciplinary professionals. The team consisted of: Department of Energy headquarters staff; RETA Security, Inc. senior personnel; Sandia

Slide presentation attached

Copyright: RETA Security, Inc. 2003

Laboratory personnel from the computer tactical simulation lab; and U.S. Army Special Forces personnel on assignment for force on force exercises. All four groups integrated their efforts through all phases of the quality assurance process to include the publication of the final reports. One of the first sites reviewed was Rocky Flats. On March 21, 1997 Col McCallum issued a classified letter to the Rocky Flats Operations Office declaring them to be at high risk. Within months, Los Alamos and the Transportation Division were also determined to be at high risk. The quality assurance team continued to review Site Safeguards and Security Plans and Vulnerability Analysis Reports through the fall of 1999 when we were disbanded by Joe Mahaley director of Office of Security for Department of Energy and Toby Johnson now acting director of nuclear safeguards and security for NNSA.

In the spring of 1998, three Department of Energy employees from the headquarters Office of Safeguards and Security and myself were assigned by Marshall Combs of headquarters Department of Energy to provide technical assistance to Peter Stockton, a special assistant for security to Secretary of Energy Bill Richardson. Over the next 18 months, until the fall of 1999, the special assistant and I prepared 13 classified white papers for the Secretary outlining a variety of security risks at the various Department of Energy sites. These papers not only disclosed vulnerabilities, but also disclosed cheating and altering of risk ratings for various sites and the transportation division by Department of Energy management.

The information, documentation, and data disclosing the high risk were passed up the chain of command from the quality assurance team and down the chain of command from Secretary Richardson. Virtually nothing was done to address the high risk even though Departmental Orders require compensatory remedial actions within 24 hours of the disclosure. Since that time we have raised these concerns with Secretary Abraham, and once again, other than denial, nothing was done to address the concerns.

Copyright: RETA Security, Inc. 2003

In the committee's letter of invitation sent to me you said the purpose of the hearing was to determine the "adequacy" of security in Department of Energy. The expression "adequate" is a layperson's term. The department has very prescriptive definitions of risk for the consequence of loss of nuclear materials and risk to the health and safety of the public. Risk in a Vulnerability Analysis report is developed as a quantitative value, that is in turn provided adjectival designations of high, moderate, or low risk. When a site is determined to be at high risk, compensatory measures must be implemented within 24 hours as I mentioned earlier. A simple red flag you should look for in a description of risk is "adequate" which in fact is an obfuscation of a risk state. Based on past Department of Energy policy and management, and my current activities in the department, I fear that we remain at high risk today. I urge you to look into this critical concern. I further urge you not to accept the canned response, "we fixed it" without clear verification. The people who long tolerated and even abetted the failings in the department are still there, with no one else to oversee their actions.

The risk of loss of nuclear materials or the risk to health and safety of the public is from adversary tactics of theft or sabotage. Theft is an action to steal enough nuclear materials to make a nuclear bomb from uranium or plutonium. Sabotage to uranium or plutonium inventories can create either an improvised nuclear device or a radiological dispersal device. The department first recognized the problem of improvised nuclear devices in 1990. I was a technical consultant on the tiger team that determined where on the various sites in Department of Energy the concern of an improvised nuclear device existed. We also recommended corrective actions to address vulnerabilities at the respective sites. Compensatory corrections where made within 24 hours at all of the affected sites. The problems of improvised nuclear device is an ongoing concern with open issues still plaguing the department today. The issue of radiological dispersal devices was not surfaced in the department until 1995 with the issuing of the Presidential Decision Directive 39. PDD-39 was later augmented with PDD 62 and 63 further addressing weapons of mass destruction. The problem of radiological dispersal devices, like improvised nuclear devices is an ongoing concern with open issues still plaguing the department today

Copyright: RETA Security, Inc. 2003

You have asked "what has the assessment shown?" The assessments, particularly the quality assurance teams efforts, documented high risk at certain sites. When for example from 1997 to 2000, over 200 classified and unclassified letters and reports were prepared by the quality assurance team, of which I was a principal author, that identified high risk to three major facilities with tons of highly enriched uranium and plutonium holdings. The assessments included theft of special nuclear materials and sabotage resulting in either an improvised nuclear device or radiological dispersal device. I personally briefed the high risk findings to Joe Mahaley and Toby Johnson. Neither one acted in accordance with Department of Energy Orders. Some of these same issues were briefed to Secretary Richardson and he staffed them to the same two persons and nothing was done to address the vulnerabilities. Members of the quality assurance team surmised that what happened in these instances was that OSS (now the Office of Security) would float the issue to the two responsible program offices, Defense Programs and Environmental Management, where there would be immediate reluctance to address the issue. There was continuous "foot dragging" by each of these program offices in regard to evaluating the consequences of loss of nuclear materials or the definitions and characteristics of the design basis threat. For example, when developing a worst case scenario, the quality assurance team would often assume to arm the terrorists with a 50 caliber sniper rifle with armor piercing incendiary rounds - the program offices would argue that this was unfair to the protective forces! Regularly, the program offices would balk at the high risk determination at a site because if they were to acknowledge the state of risk they would have to fix it and institute immediate compensatory measures and that would divert funds from programmatic efforts. Why was there no action? There are a variety of explanations to include:

- culpability - management would have to acknowledge past problems
- cost potential - large expenditures to fund operating dollars for increased security forces and facility dollars for hardware
- politically incorrect - those who subscribe to the problem have disappeared through reassignments.

Copyright: RETA Security, Inc. 2003

How is risk assessed? The department uses a standard risk equation developed in the early 70s. The equation for risk (R) is:

$$R = C \times T \times (1 - PE).$$

- The term "C" is the value of consequence of loss used for theft or sabotage of nuclear materials and danger to the health and safety of the public.
- "T" is a value assigned to the design basis threat, such as terrorists
- PE is a value for the basic elements of a physical security systems used at the sites in Department of Energy to protect the nuclear assets and consists of detection, delay and response.

In and of itself the equation for risk is algebraically simple, perhaps deceptively so. For example, in physics the equations developed by Newton and Einstein, $F = ma$ and $E = mc^2$, are also simple. However, one determines space flight and one develops nuclear weapons. The risk equation in Department of Energy is used to determine the protection required for assets of societal importance, i.e., theft or sabotage of nuclear materials from the national inventory under the stewardship of the Department of Energy.

It is important to note that when determining risk the protection effectiveness "PE" term is TIME sensitive. Terrorists, whose goal may be theft or sabotage, want to minimize their time to accomplish their objective. For example, a time line tested at a Department of Energy site was 34 seconds to steal 20 Kgs (44 lbs) of high grade uranium! The determinant factor in thwarting a terrorist act is the ability of the site's protective force to interrupt and neutralize the terrorist. Simply put, can the protective force kill the terrorist before the terrorist is successful? We failed the TIME trial on the USS Cole and at the Dahran barracks just to name a few recent examples of national failures in security when we were on high alert to terrorist acts.

Today, the department has no "KILL" standard. Historically, we have seen guard forces sized and equipped with the "last man standing" criteria. This criteria means we have a guard force with just enough capabilities so that in a engagement between the terrorists and the protective forces the

Copyright: RETA Security, Inc. 2003

protective force will have one man left after the battle! During the quality assurance effort, we proposed a definition for a robust guard force protecting against theft or sabotage that included such basic elements as: guard force size per shift; tactics of denial, containment, recapture, recovery; and armament. No standard policy exists today for what a margin of prudence is necessary for a protective force to ensure the protection of nuclear materials. If you need more guards to ensure a win with a margin of error, their cost is an overhead operating budget item which will reduce programmatic efforts. If we don't subscribe to the reality of a terrorist act, minimal dollars will continue to be set aside for protection in the nuclear weapons complex. The existing protective force management in the department does not allow any margin of error.

The continued concern for protection of nuclear materials and the safety of the public resulted in my writing a confidential letter to the "czar" of security for the Department of Energy in January 2000 expressing my concerns and accusing Joe Mahaley and Toby Johnson of lying about the state of security in Department of Energy and the high risk to theft and sabotage of nuclear materials. The "czar" never contacted me about my allegations, but simply turned my letter over to the Inspector General's Office. After 10 months the IG said it could find nothing to refute the "high risk" determination contained in the 200 unclassified and classified documents given to them. Because the accusation of "lying" could not be proven, the crucial charges were dropped with the contention that management was aware of the high risk. To paraphrase a recent quote from Steve Wallace of the Columbia Accident Investigation Board "what seems to have evolved is that higher-level decision makers came to the conclusion that there *isn't a security* issue in part based on an analysis done by analysts who sort of wanted *low risk.*[1]" In January 2001 I approached the Project On Government Oversight (POGO) and together with Peter Stockton, the special assistant to Secretary Richardson, we co-authored a report "US Nuclear Weapons Complex: Security at Risk." This report detailed the high risk in the department's nuclear weapons complex. The report was 99% complete on 9/11/01 when the greatest terrorist act against this nation occurred. The Department of Energy

[1] Tribune Newspapers, Michael Cabbage, 6/6/03.

Copyright: RETA Security, Inc. 2003

complex was at high risk then against a much simpler terrorist design basis threat than used in the actual attack on 9/11, or that used most recently in the Riyadh compound attack.

Nineteen months after the September 11th attack, a new design basis threat was finally issued on May 28, 2003. A draft version had been circulated on 12/31/02 that included an increase in the number of terrorists **and** a lowering in the numerical value for low risk. The draft design basis threat would have approved one failure in every 20 attacks to be at low risk. Today's new design basis threat approves a considerably higher rate of loss. It is the same rate used before the 9/11 attack. On 9/11 the terrorists succeeded in three out of four attempts. Either an addition to the number of terrorists **or** a decrease in the approved low risk would result in a linear increase in the size of the protective force for a given site. By making just one change to the design basis threat, the security improvements are simplified. Even with the new and simple changes to the design basis threat, the necessary implementation schedule for funding of security improvements are not required to be completed until 2009 with the actual implementation to follow some time later!

The department has been at risk to theft and sabotage since 1997 to a simpler threat that was often "dumbed down" by program offices. For example, please recall the hew and cry about 50 caliber sniper rifles referred to earlier in this testimony. Today, we are at an even greater risk with any increase in the design basis threat whether it is increased numbers of terrorists or the reduction in the value of low risk. The increase in the number of adversaries results in the need for timely response of the protective force with two to three times more personnel for each "new" adversary. If the approved risk is lowered, the same type of increases to the protective force size is also needed. Funding, hiring and training of a larger protective force takes at least 18 months. Livermore Labs disbanded their special response teams in 1995, when it was pointed out to them that they were at high risk in 1997, it took them 18 months to reconstitute the force.

I have talked about the risk to the nuclear weapons complex in the department and the risk to the health and safety of the public as well as the lack of corrective action for a just approved design basis

Copyright: RETA Security, Inc. 2003

threat, but how do we fix it? There is no quick fix in a department that has been dysfunctional[2] as long as the Department of Energy has, but there are corrective steps to start the improvement process. The are:

- Hold senior managers in the department accountable for their actions. Many of the current managers in the department knew and know about high risk to the nuclear inventory from theft or sabotage and they were given thousands of pages of classified reports documenting the high risk. To date reorganization of the department, to include NNSA, has only rearranged the deck chairs. We need to replace these persons with qualified personnel. The bureaucrats in place protect one another. You can't expect friends to fire one another. In this case only the congress can affect change. Top leaders should be held accountable. Their action should put their careers on the line. Today, one of the aforementioned Department of Energy directors has been given an award and the other is at Lawrence Livermore Laboratory looking into the security failure of the lost security keys! What we need are qualified persons with experience in loss-prevention, not simply retired military persons whose experience is in national defense or law enforcement.
- Consolidate the nuclear materials to central repositories in a timely manner. Secretary Richardson, before he left, signed a Decision Directive to move nuclear materials from Los Alamos. It is still being planned three years later with the movement of nuclear materials on a distant horizon. This is an example of malicious compliance by current departmental managers and program offices.
- Provide line item funding for physical security at the level of a program offices to include operating dollars designated for increased protective forces size and capabilities. Today the Department of Homeland Security has a budget greater than $30B. However, Department of Energy management resists spending money on security. If they establish a new 24/7 post or patrol for the protective force at any of the Class A sites, this is equal to about five full time protective force personnel which is the same cost as two or three scientists. Therefore

[2]Special Investigative Panel of the President's Foreign Intelligence Advisory Board. June 1999.

Copyright: RETA Security, Inc. 2003

the scientist must be laid off to hire the security personnel - not a popular option. The program offices have an inherent conflict of interest when deciding to improve security and lower risk or lay off scientists.

This panel has diverse backgrounds, professional training, and expertise, but we have arrived at the inescapable conclusion that the Department of Energy weapons complex is at risk.

POGO has gathered and assimilated a lot of information from informants and whistle blowers that has been thoroughly examined and summarized to determine the status of security in the Department of Energy complex to include not only concerns about theft and sabotage to nuclear materials, but also espionage and fraud.

My corporation, along with other professionals from Department of Energy, Sandia and the Army's special forces have exhaustively documented departmental vulnerabilities during the quality assurance effort. They have provided practical input to worst case scenario development and they have tested and stressed protective forces in the complex with force on force testing. They have helped address weaknesses in: tactics, armament, and size of the protective forces. Through the use of surprise, violence of action, and fast time-lines they can fully exploit vulnerabilities and then prescribe actions to correct the weaknesses and vulnerabilities.

The information presented by this panel to you was developed from diverse sources which agree that Department of Energy is doing too little too late to address the risk in the complex.

In conclusion, let me summarize my testimony. Many of the nuclear weapons facilities in the Department of Energy are at risk which endangers the health and safety of the public. This has been documented continuously since March 1997. The security for the nation's nuclear stockpile has been mis-characterized as "adequate" by career senior personnel within the department. The corrections and remedies for the existing problems falls to Congress for action.

Purpose of Hearing: Examine the "adequacy" of security in DOE the term ***adequate*** is a "red flag"

- DOE Orders expressly determine quantitative risk to assets of societal value (loss of nuclear material, health and safety of the public). The risk has adjectival ratings of high, moderate, low.
- Significant Assets:
  - Theft of bomb grade quantities Uranium and Plutonium
  - Sabotage of: Improvised Nuclear Device (IND), Radiological Dispersal Device (RDD)
- Risk to the health and safety of the public

What have assessments shown?

- Extensively documented High Risk of theft and sabotage to DOE's nuclear inventory since March 21, 1997.
- Extensive QA/QC program in past included:
  - DOE headquarters personnel
  - RETA Security, Inc. Analysis
  - Sandia National Laboratory Simulations
  - Army Special Forces Testing
- Interference by Program Offices

How is risk "R" assessed?

$\downarrow R = C \times T \times (1 - PE \uparrow)$

C is the consequence of loss or importance of the asset

T is the design basis threat

PE is physical security: detection, delay, response

- PE is ***TIME*** sensitive with final determinant based on the response force – interrupt and kill
- No "kill" standard to validate risk "R"
  - last man standing for protection of societal assets!

Design Basis Threat (DBT)

$R = C \times T \times (1 - PE)$

Where the threat (T) is the Design Basis Threat (DBT)

- No change in DBT from 9/11/01 for 19+ months!
- New DBT of 5/28/03 will:
  - Increase number of adversaries
  - No change in value of low risk
- Implementation to begin in FY-05, funding not completed until FY-09!
- Major impact on response force!!

Remedies

- Accountability – none today, no oversight
- Fast track consolidation of nuclear inventory
- Line item funding for physical security
  - Today there is dilution of funds by programmatic offices with security treated as an overhead item
  - DP, EM dilemma: hire security - fire scientists

Mr. TURNER. We thank both of you.

We will have a 5-minute round of questions beginning with Chairman Shays.

Mr. SHAYS. Thank you very much.

Ms. Brian, I appreciated both your testimonies. I appreciated your testimony in terms of helping us raise some questions behind the closed door. Some of them, frankly, could have been raised not behind closed doors, and we should have asked about the issue of intimidation and so on. So it will be on the record behind the closed doors, but it is not really confidential information.

I wrote down that what I was trying to wrestle with, a breach in terms of the force-on-force exercise, a breach success, a facility is vulnerable. We can know that if you are going to tell them that you're going to attack and you allow both sides to plan for the offense and defense and you still succeed in getting through, you've got a big problem.

Ms. BRIAN. That's how we see it.

Mr. SHAYS. A nonbreach does not suggest the facility is not vulnerable because they have been warned. That was kind of what I was wrestling with and suggesting.

Ms. BRIAN. I thought that was a great point you were making, and I thought you——

Mr. SHAYS. I didn't make it well though.

Ms. BRIAN. Well, make it again in the closed session. But I think that actually what you were encountering is important. You saw the defense of the status quo on the part of Mr. Mahaley in not wanting to—when you said, "Why are you disagreeing with me?" I mean, I thought that was a very important dialog that you had with him, that at DOE they don't want to acknowledge weaknesses in the way the system works.

Mr. SHAYS. In terms of your information, how many times in the last few years have we been able to breach a facility?

Ms. BRIAN. Our understanding is that over 50 percent of the time the mock terrorists in "full up"—this means the independent, full DOE assessments, not the self-assessments that are done by the labs for themselves, the facilities for themselves, but in the big, "full up" ones—more than 50 percent of the time the mock terrorists are successful at achieving their mission, whether it be theft or creating, as we discussed before, you know, the improvised nuclear device, whatever their mission is.

Mr. SHAYS. Both of you can respond to this. Based on your work and research and knowledge, what facilities do you think are the most vulnerable?

Ms. BRIAN. I can't know that because I don't have a clearance. And the only examples that I know of are those that have been—the security failures that have been fixed, and that's the way I'm able to know those.

But I can specifically speak to one facility, TA 18, which has been identified by the last two administrations as being the most vulnerable. It's at Los Alamos; and as I mentioned, Secretary Richardson ordered that it be deinventoried of all of its special nuclear materials by now, and none of it has moved out yet.

And there's all kinds of excuses coming from Los Alamos—we're not ready yet. And this administration actually issued a stern

warning that they needed to get the stuff out. It's in a canyon. So the high ground—the bad guys can have the high ground and we all know from, you know, cowboys and Indians, that's not the way you want to be storing special nuclear materials.

Mr. TIMM. In fact, one of the characteristic stories of that site was the fact that they dumbed down the tests and told the Special Forces people when they were stealing material—I think it was in 1997—that they couldn't use a vehicle, and they went and brought in a garden cart, because that wasn't prohibited; and then they were able to steal the material. And they yelled, "Foul," that it was not a reasonable test because they used a garden cart to drag away the SNM. So that's some of the artificiality that you see going into those force-on-force tests.

Force-on-force tests are not cheap, sir. They run anywhere between $100,000 and a quarter of a million dollars to pull one up and run it; and labs are very reluctant to go ahead and put that kind of money into it.

Mr. SHAYS. I happen to think they are tremendously important—but not to enable the Department to say that "We've done this, so we know this facility is safe." It's a wonderful tool for everyone to know the vulnerabilities and how they can then try to prevent them in the future.

If you were to ask any of the participants in the closed-door session a question, give me your top few, both of you.

Ms. BRIAN. Well, one that I wrote down, that I wish I could, is when you were asking—I think it was maybe you, Mr. Tierney, who asked Ambassador Brooks, "Do you believe that you have been able to reach denial—in other words, the ability to stop the terrorists from coming in the site"—and he said, "Absolutely, yes, we've reached that capacity." And you asked, "Well, how do you know that?" And he said, "Well, because of this force-on-force test."

I would encourage you to ask Mr. Podonsky or the GAO whether force-on-force tests of denial have been run at all of these facilities and whether it has been successful in preventing the terrorists from getting in.

I don't believe the answer would support Mr. Brooks's, Ambassador Brooks's testimony.

Mr. SHAYS. Thank you.

Mr. Timm.

Mr. TIMM. I think I would ask the question about how much have they actually done, performance testing, against the RDD. In that when you take a weapon of mass destruction, a truck—and, in fact, there are trucks—bomb size is classified, but if you talk to the Technical Security Working Group for the Department of Defense, they classify it as a 60,000-pound vehicle. If you parked it next to a building, which we postulated, outside of Denver and blew that up, you would basically have taken that plutonium and wafted it over the city of Denver.

And so the question is, do they really test weapons of mass destruction to, in fact, implement an RDD at those specific sites.

We didn't find vehicle barriers along fences, so in fact the bad guy could cut them without anyone even watching them and then drive that 18-wheeler right up alongside of a building. That's all you'd have to——

Mr. SHAYS. I missed what you said. Please say that more slowly. You did what?

Mr. TIMM. We postulated driving an 18-wheeler right up next to a building and exploding it with whatever poundage of high explosives in it, which would then waft the plutonium in this particular site up into the air and it would have blown over the city of Denver, and did not test against the RDD, as to my best knowledge, and I work with the Department actively.

Mr. SHAYS. We'll check that out as well.

Any other questions that you think would be wise to ask, if you'd submit them to our staff before 2 today, I think we'll do that.

Mr. TIMM. OK.

Mr. SHAYS. Thank you both very much. Appreciate your work and appreciate your testimony, and my only disappointment was that you pointed out a question, too, that we could have asked in public that I wish we had.

Thank you, Mr. Chairman.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. Tierney.

Mr. TIERNEY. Thank you, Mr. Chairman.

And I thank both of you for your testimony. My only regret is that we didn't arrange this testimony differently and have you folks testify first so that we would have been able to see the reaction and the commentary from the others in a public session, at least as much as we could. And I might recommend to my colleagues on the other side that we all go back and think about the way we structure these witnesses from time to time, because that might be helpful; and hopefully that's something we'll consider.

I get concerned because when we had the hearings on the Nuclear Regulatory Commission and the protection of nuclear power plants, we heard the same stuff—you know, the inadequate force-to-force test, the inadequate threat design, and it goes on and on. And I know I get criticized in my area from the people in the nuclear industry, who keep thinking that we're being overly aggressive in our research of them, and that they think they're all safe. But when you visit those plants, you see all the things that the tests show.

We hear port security commentary. We still haven't even set the idea of what we need to do to prioritize what can be done, although we all know from other independents that have done that, that we could do things. We know, still, that like 42 percent of the cargo in passenger planes is not screened, and—it's incredible. And we still know that we don't have a proper communications coordination system going around here with all those things that are available.

And I know that others, and I, are putting together a system of where we should be on all of those points at a certain time; and hopefully, we can hold this administration to that point, because it really gets to the point of ridiculousness when we see what's going on.

Ms. Brian, you mentioned that we ought to think possibly about putting the Department of Defense in charge of security at these facilities. The current security obviously is private individuals, and

they're either inept or there's some other explanation for why they're not doing the job.

But is the Department of Defense going to have the kind of expertise, as Mr. Timm mentioned, that sometimes just bringing in the brass doesn't resolve it? Or should we go to a wholly separate group of real specialists and establish them to do it?

Ms. BRIAN. Well, actually what I was suggesting—and perhaps I wasn't clear—was not to have the security itself run by DOD. I think actually NM posse comitatus may prevent us from doing that. But I meant the oversight of the security.

And one way of doing that is—well, there are parts of DOD, not just people who have things on their shoulders, but who are actually trained. And one of the many places that we actually briefed with our findings was the Nuclear Control and Command staff, and it struck me that their job is the security and oversight of the security of the DOD nuclear weapons themselves, and so they already have that level of training and expertise.

And they are tremendously critical of DOE, and frankly, I thought that perhaps by taking advantage to some extent of the interagency rivalries, if you had someone who really was trying to find where the problems are, we would actually improve security.

Mr. TIERNEY. Is this a question of the Department of Energy knowing what they should have to do and not being willing to spend the money or appropriate the resources to it, or is this just a question of flat-out incompetence?

Ms. BRIAN. I think maybe it's both of those, plus a level of bureaucratic inertia that people don't want to change the way they have done things, and they certainly don't want to admit that they have been wrong.

You have a lot of the same people in place, as Mr. Timm mentioned. When the NNSA was created, we actually had as an attachment to our report the press release announcing the new NNSA and the people who were going to be in this new job. Well, they were all the same people who had been at the DOE defense programs, and they just changed their title. So I think a lot of it is, frankly, people who are still there and don't want to—you know, who sort of dig in their heels and say, no, the outside critics are wrong; we know what we are doing. So I think that's a lot of it.

Mr. TIERNEY. Thank you.

Mr. Chairman, can we have that POGO report made a part of the record, unanimous consent?

Mr. TURNER. Sure, without objection.

Mr. TIERNEY. Thank you.

And last, just the design basis threat, Mr. Timm, you started to talk about that a little bit. Can you give me your evaluation of that most recent document?

Mr. TIMM. I think there was a characterization that it was what money could buy. The one they had on December 31, the draft one, in fact, I thought was aggressive. I thought it was responsive and I thought it did meet the mark on that. And I was surprised at the robustness of it, because they increased not only the number of terrorists coming, but also said, we're going to accept less risk at the site. And that was an important element that they added to that.

It was going to have—people have to change a lot of ways they think as with regards to, you can't just throw people at the problem anymore. You've got to get a lot smarter than what they do. And so they basically—again, we have beaten to death the words "dumbed down," but they basically dialed it down to where it was an acceptable function.

Mr. TIERNEY. And you think they did that for financial reasons?

Mr. TIMM. Absolutely. Absolutely. It's no question that they had to because of the amount of manpower you would have to bring to bear, or even changes in tactics that you would have had to accomplish within that function.

Mr. TIERNEY. Thank you both for your testimony. It's valuable to us.

Ms. BRIAN. Thank you, sir.

Mr. TURNER. Looking at your testimony, Ms. Brian, when you indicated the options that could be pursued, the one obviously with the Department of Defense having responsibility is the one I think that intuitively most people would arrive at, and maybe even begin there.

If you ask people, who is guarding these facilities, I think most people's perception would be that the military is not, and not that we have Department of Energy or even contractors that are participating in that.

Mr. Timm, in looking at your testimony, you state that one of the concerns that you have is that what we need are qualified persons with experience within loss prevention, not simply retired military personnel whose experience is in national defense or law enforcement. I mean, that obviously seems like a conflict, and I would just like you guys to discuss that for a moment, because it would seem to me, Ms. Brian, that your statement is one that is—as you went through what the Department of Defense does in security and other facilities, it seems like this would be a natural fit—and if you both would discuss that issue.

Mr. TIMM. I don't think we are in disagreement at all. It may have been the wording that we chose on this.

The Department of Defense, as far as command structure, ability to train and have people available to do that, is obviously a ready source of manpower. At Livermore Laboratory it took them a year and a half to reconstitute their SRT after they had disbanded it in 1995. And so I don't see a problem with that.

The problem you have, when I talked about bringing command structure people in here is, they bring in the military aspect of how they look at it, and it is a national defense perspective rather than loss prevention.

I have worked with many competent people out of the Defense Department that are perfectly capable of doing this within the construct of what you're trying to put together.

And so I don't believe we are there. It's just a matter of the devil's in the details as far as pulling these two together.

Ms. BRIAN. And I think also the distinction is rather than having someone at the top who has not had experience actually protecting assets but has another entirely different—as was suggested there, admirals who I think have strategic command experience; it's not the same kind of military experience that many of the Special

Forces—for example, there's a unit out of Fort Bragg that is trained of special operations—that is trained specifically as adversaries. And that's what they do. And they go to different sites and train and try to breach security.

And those are the kinds of people that we're talking about being involved rather than people who have a military career but have nothing to do with actual, you know, entering—being pretend terrorists, mock terrorists or, you know, protecting assets.

Mr. TIMM. In fact, the experience I had personally was with a one-star general who was head of MPs, that retired and went to the Department of Energy at Oak Ridge, and I spent quite some time explaining our equation to him so that he understood. We would walk out there and test up. He would say, well, show me what you mean, Ron, by doing X, Y and Z. We would cross fence lines and find out that the fence line didn't work the way it was supposed to, and he would immediately stop and go into compensatory modes. We one time stole some materiel out. It was gone over the fence in 34 seconds, but that command general was capable of dropping back and saying, this is what I don't know, and this is what I need to know about loss prevention.

So it's not to say they're dumb at all. It's to say their experience is not in the area of loss prevention. It's in national defense.

Mr. TURNER. Very good. As you know, we're going to be adjourning to a closed session at 2 p.m. Do you have anything else that you would like to add at——

Mr. TIMM. No. As far as I understand it, I'm invited to the 2 o'clock session because I have a clearance.

Mr. TURNER. Yes. My statement was do you have anything else that you want to add in this public portion of the hearing.

Mr. TIMM. No.

Mr. TURNER. I ask for unanimous consent that the subcommittee meet in closed session at 2 p.m. today to hear testimony on classified aspects of issues under discussion today. And, without objection, it is so ordered. Thank you.

[Whereupon, at 12:10 p.m., the subcommittee proceeded in Closed Session.]

[Additional information submitted for the hearing record follows:]

Department of Energy
Washington, DC 20585

July 16, 2003

The Honorable Christopher Shays
Chairman, Subcommittee on National Security,
Emerging Threats, and International Relations
Committee on Government Reform
United States House of Representatives
Washington, DC 20515-6143

Dear Chairman Shays:

Thank you again for giving us the opportunity to testify before the Subcommittee on National Security, Emerging Threats, and International Relations on June 24, 2003.

During the closed session, you offered me and my colleagues the opportunity to provide written public statements in response to Mr. Ronald Timm's testimony to be appended to the open hearing record.

Please find enclosed statements from me; Larry Wilcher, Director, Security Policy Staff, Office of Security; and Samuel Callahan, Program Manager, Strategic Threat Assessment and Vulnerability Analysis, Security Policy Staff, Office of Security.

Sincerely,

Joseph S. Mahaley
Director
Office of Security

Enclosures

Printed with soy ink on recycled paper

Public Statement of Joseph S. Mahaley,
Director, Office of Security,
U.S. Department of Energy, in
Response to Testimony of
Ronald E. Timm, Certified Protection Professional
President, RETA Security, Inc.
to the 108th Congress, House of Representatives
Committee on Government Reform
Subcommittee on National Security, Emerging Threats and International Relations
June 24, 2003

Regarding Mr. Timm's assertion on page 1 of his testimony that "[a]fter making [his] concerns about inadequate security [sic] to Department of Energy headquarters, and the current administration, [his] headquarters work was terminated."

Mr. Timm's contract relationship with the Department was not terminated. Options for additional work were not exercised. I had no role whatsoever in any decision regarding those options. To the best of my knowledge, none of the DOE political appointees in the current Administration that I report to had any role in any decision regarding those options.

I did however, receive a report regarding Mr. Timm's work after Edward McCallum, the Director of the Office of Safeguards and Security (OSS) and my subordinate, was detailed to the Department of Defense in 2000. Mr. McCallum was also a lieutenant colonel in the Army Reserve, where I believe at some time he had become acquainted with Mr. Timm, who I believe had been or was a sergeant in the Army Reserve.

The new director of the Field Operations Division of OSS, Mr. Jim Ford, reported to me and Mr. Toby Johnson, acting OSS Director, that he was concerned about the large amounts of funds being committed to Mr. Timm and his son-in-law, doing business as RETA Security, Inc. Specifically, I was informed that almost $900,000 had been paid to Mr. Timm and his son-in-law over 27 months. When Mr. Ford asked his subordinates why RETA Security, Inc., had been paid so much, he was told simply "F.O.E." When I asked Mr. Ford what F.O.E. stood for, he said "Friend of Ed" meaning Mr. McCallum. I directed that any support service contract decisions should be based on legitimate government requirements and priorities and not based on personal preferences for old friends. We reported this to the Office of Inspector General, and they informed us they had received prior complaints on the preference issue regarding Mr. Timm's work in OSS. They informed us they had determined to take no action and that we were free to handle the situation administratively. Besides directing the end of the preferential treatment that had been reported to me, I took no other action regarding Mr. Timm's support service contract at any time.

Regarding his assertion on page 2 that "[t]he quality assurance team continued to review Site Safeguards and Security Plans and Vulnerability Analysis Reports through the fall of 1999 when we were disbanded by Joe Mahaley director of Office of Security for Department of Energy and Toby Johnson now acting director of nuclear safeguards and security for NNSA."

The decision to terminate quality assurance team activity was made by then Under Secretary of Energy, Ernest Muniz, and my predecessor, General Eugene Habiger, because of the 1999 enactment of the National Nuclear Security Administration (NNSA) Act and the Department's decision to implement a new Site Safeguards and Security Plan development process. I had no direct role in "disbanding" the quality assurance team's work. However, I believe there was no legal alternative after Congress, in the NNSA Act, stripped Department of Energy employees of any authority over NNSA employees.

Regarding his statement on page 4 that he "...personally briefed the high risk findings to Joe Mahaley and Toby Johnson. Neither one acted in accordance with Department of Energy Orders. Some of these same issues were briefed to Secretary Richardson and he staffed them to the same two persons and nothing was done to address the vulnerabilities."

Mr. Timm's assertion that I have not acted in accordance with DOE Orders is false. I have always acted in accordance with DOE Orders and lawful direction from the Secretary of Energy. I recall only one briefing I personally received from Mr. Timm while he was providing support services to OSS. He briefed me on vulnerabilities regarding DOE's Transportation Safeguards Division, now redesignated the Office of Secure Transportation. Contrary to his assertion, the DOE acted on his and other information concerning TSD problems, focused management attention, and committed over $60 million dollars to correct them. The DOE's Transportation operations have been significantly improved as a result of that and subsequent initiatives. I personally reported the problems regarding TSD to the senior leadership at DOE and they were subsequently reported to the President. I personally briefed the President's Counterterrorism Coordinator on the reported problems and corrective actions.

Regarding his assertion on page 6 that I had lied "...about the state of security in Department of Energy and the high risk to theft and sabotage of nuclear materials."

Mr. Timm's assertion is false. I strongly object to Mr. Timm's characterization that I lied about the state of security in the Department of Energy or mischaracterized the level of risk to our nuclear materials.

I am particularly and personally offended by this false assertion by Mr. Timm because I have always done precisely the opposite of what Mr. Timm asserts – I have always reported the truth to my political superiors without regard to their possible displeasure or other consequences. As a

matter of fact, I still have personal litigation pending against the DOE because of unlawful retaliation taken against me by a Secretary of Energy during the Clinton Administration for my telling the Secretary his directions regarding a hiring action violated the law. I did this without any support from DOE's Office of General Counsel, Office of Human Resources, and Office of Civil Rights, whose leaders, although present, remained silent when I so informed the Secretary. I have maintained my integrity at heavy cost to myself and my family, and I will not suffer Mr. Timm's defamation in silence.

Public statement of Larry D. Wilcher
Director, Security Policy Staff
Office of Security
U.S. Department of Energy
Response to Testimony of
Ronald E. Timm, President RETA Security, Inc.
to the 108th Congress House of Representatives
Subcommittee on National Security, Emerging Threats and International Relations
June 24, 2003

Regarding Mr. Timm's assertion on page 1 of his testimony that "After making my concerns about inadequate security to Department of Energy headquarters, and the current administration, my headquarters work was terminated."

Mr. Timm's contract relationship with the Department of Energy was not terminated. As the former Director, Field Operations Division, Office of Safegaurds and Security, I chose not to exercise an option to continue work under that portion of the contract which was being performed by RETA, inc. I was never directed to terminate Mr. Timm, nor RETA, Inc. I made the decision based on the fact that the Site Safeguards and Security Plan (SSSP) validation work performed by RETA, Inc. was no longer required. Prior to my assumption of the position as Director, Field Operations Division, the Undersecretary of Energy, Ernest Muniz made a decision to implement a new SSSP process. This new process eliminated the role of the Office of Safeguards and Security as a quality assurance review team for developing SSSPs and hence the SSSP validation process. I therefore made the decision not to exercise this subtask on the existing support service contract.

Public Statement of Samuel N. Callahan,
Program Manager, Strategic Threat Assessment and Vulnerability Analysis,
Safeguards and Security Policy, Security Policy Staff,
Office of Security, U.S. Department of Energy, in
Response to Testimony of
Ronald E. Timm, Certified Protection Professional
President, RETA Security, Inc.
to the 108th Congress, House of Representatives
Committee on Government Reform
Subcommittee on National Security, Emerging Threats and International Relations
June 24, 2003

Regarding Mr. Timm's assertion on page 3 that "[t]he issue of radiological dispersal devices was not surfaced within the department until 1995 with the issuing of the Presidential Decision Directive 39."

The assertion that the Department did not consider and protect against radiological dispersion is inaccurate. The Department of Energy has had an established, formalized safeguards and security vulnerability assessment process since 1987. A key factor in the conduct of the vulnerability assessment process has been and continues to be consideration of radiological sabotage events.

Regarding Mr. Timm's assertion on page 7 that "Nineteen months after the September 11th attack, new design basis threat was finally issued on May 28, 2003."

The "Department of Energy Design Basis Threat Policy" was formally approved on May 20, 2003. The Department took positive measures to enhance the protection afforded national security assets at its facilities immediately following the events of September 11th 2003. The Secretary of Energy issued a memorandum October 3, 2001, increasing/augmenting the protection strategy to be employed at Departmental facilities that process, store, transport or handle significant quantities of Special Nuclear Materials. The Director, Office of Security, issued a memorandum January 11, 2002, that initially advanced the concept of a graded threat and the realization that the then current design basis threat (FY 1999) would need to be revised to incorporate emerging world threats. The 2003 design basis threat incorporates the concepts and requirements initially published in the October 3, 2001, and the January 11, 2002, memorandums.

Regarding Mr. Timm's assertion on page 7 that "[a] draft version had been circulated on 12/31/02 that included an increase in the number of terrorists and a lowering in the numerical value for low risk. The draft design basis threat would have approved one failure in every 20 attacks to be at low risk. Today's new design basis threat approves a considerably higher rate of loss."

Mr. Timm's assertion is misleading. The Departmental design basis threat policy is constructed to provide sufficient information to programs and programmatic officials to

identify the credible threats to Departmental assets so appropriate safeguards and security measures can be employed. As such, the design basis threat document is not the correct mechanism to promulgate changes in the base Departmental risk assessment methodology. Correspondingly, the revised safeguards and security system effectiveness equations and evaluation criteria are being incorporated into Departmental safeguards and security policy (Department of Energy Order 470.1).

The 2003 design basis threat does not approve a considerably higher rate of loss as the design basis threat does not address the safeguards and security system effectiveness issue at all. Rather, the Department of Energy Order 470.1 is being revised and will address the issue. However, the basic tenets of the draft design basis threat dated 12/31/02 are being included in the draft safeguards and security policy.