AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

NUCLEAR SECURITY: CAN DOE MEET FACILITY SECURITY REQUIREMENTS? (PART II)

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

SECOND SESSION

JUNE 22, 2004

Serial No. 108–237

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

97–131 PDF WASHINGTON : 2004

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
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
PATRICK J. TIBERI, Ohio
KATHERINE HARRIS, Florida

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
BETTY MCCOLLUM, Minnesota

BERNARD SANDERS, Vermont (Independent)

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

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
KATHERINE HARRIS, Florida

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
JOHN F. TIERNEY, Massachusetts
DIANE E. WATSON, California

EX OFFICIO

TOM DAVIS, Virginia
HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
J. VINCENT CHASE, *Chief Investigator*
ROBERT A. BRIGGS, *Clerk*
ANDREW SU, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on June 22, 2004	1
Statement of:	
Garman, David, Under Secretary, Office of Energy, Science and Environment, Department of Energy; and Glenn S. Podonsky, Director, Office of Security and Safety Performance Assurance, Department of Energy	052
Nazzaro, Robin M., Director, Natural Resources and Environment, U.S. General Accounting Office, accompanied by Jonathan Gill, Senior Analyst, Natural Resources and Environment; and Danielle Brian, executive director, Project on Government Oversight	13
Letters, statements, etc., submitted for the record by:	
Brian, Danielle, executive director, Project on Government Oversight, prepared statement of	32
Garman, David, Under Secretary, Office of Energy, Science and Environment, Department of Energy, prepared statement of	54
Kucinich, Hon. Dennis J., a Representative in Congress from the State of Ohio, prepared statement of	7
Nazzaro, Robin M., Director, Natural Resources and Environment, U.S. General Accounting Office, prepared statement of	16
Podonsky, Glenn S., Director, Office of Security and Safety Performance Assurance, Department of Energy, prepared statement of	67
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of	3

NUCLEAR SECURITY: CAN DOE MEET FACILITY SECURITY REQUIREMENTS? (PART II)

TUESDAY, JUNE 22, 2004

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 10:08 a.m., in room 2154, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Turner, Duncan, Kucinich, Maloney, Ruppersberger, Tierney, and Watson.

Staff present: Lawrence Halloran, staff director and counsel; J. Vincent Chase, chief investigator; Robert Briggs, clerk; Will Knight, intern; Andrew Su, minority professional staff member; and Cecelia Morton, minority office manager.

Mr. SHAYS. A quorum being present, the Subcommittee on National Security, Emerging Threats and International Relations hearing entitled, "Nuclear Security: Can DOE Meet Facility Security Requirements? (Part II)" is called to order.

This is our third hearing on Department of Energy [DOE] efforts to secure the Nation's far-flung nuclear weapons complex against the threat of terrorism. Previous testimony described substantial institutional, technical and fiscal challenges faced by efforts to develop and implement the strengthened security standard called the design basis threat [DBT].

The General Accounting Office [GAO] reported it took too long to formulate the new DBT, that it fails to capture some elements of the threat, and that the lack of a Department-wide strategy means implementation will take longer and cost more than planned. Nevertheless, witnesses pointed to tangible progress toward consolidation of nuclear material and strategies to deny even determined terrorists any access to weapons components.

But we did not hear testimony on the status of physical security enhancements at the five sites outside the active weapons complex managed by the Department's Office of Energy, Science and Environment [ESE]. As the DOE National Security Administration [NNSA] succeeds in hardening current weapons production facilities and labs, ESE sites could pose increased risk as the next tier of soft targets for terrorists following the path of least resistance.

While recent consolidation of DOE-wide security policy and oversight functions offers the prospect of consistent DBT implementation, GAO today reports ESE sites face some unique challenges

keeping pace with their NNSA counterparts. Reassessment of the risk that highly enriched uranium or plutonium at ESE sites might be fabricated into an improved nuclear device could render current security plans inadequate. Any revision to the DBT could trigger a time-consuming reassessment of all security plans. Already, the pace and cost of security strategies seem so uncertain that one site requested no funding at all for DBT implementation this fiscal year.

The good news is the stringent requirements of the new DBT appear to have transformed possession of special nuclear materials from a prestigious credential to a serious liability. Facilities now have a powerful incentive to blend down or consolidate dangerous stocks. But complex management structures, jurisdictional stovepipes and the resultant lack of clear lines of authority for clear DBT-related activities create unique barriers to strengthening security at ESE sites. And answering the vexing question "How much security can we afford?" becomes even more difficult when evaluating the cost/benefit yield of capital improvements and security enhancements at decommissioned facilities DOE hopes to close sooner than later.

We are grateful for the time and expertise made available to the subcommittee today by representatives from the Department of Energy, the General Accounting Office, and the Project on Government Oversight. We particularly appreciate the patience and forbearance of our DOE witnesses who agreed to forgo their customary place on the first panel. Their forbearance and willingness to listen will allow them, and us, to engage in more meaningful and constructive dialog.

[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
[illegible]K E. SOUDER, INDIANA
[illegible]EN C. LaTOURETTE, OHIO
[illegible]G OSE, CALIFORNIA
[illegible]N 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
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
MARSHA BLACKBURN, TENNESSEE
PATRICK J. TIBERI, OHIO
KATHERINE HARRIS, FLORIDA

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

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

Statement of Rep. Christopher Shays
June 22, 2004

This is our third hearing on Department of Energy (DOE) efforts to secure the nation's far-flung nuclear weapons complex against the threat of terrorism. Previous testimony described substantial institutional, technical and fiscal challenges faced by efforts to develop and implement the strengthened security standard called the "Design Basis Threat" (or "DBT").

The General Accounting Office (GAO) reported it took too long to formulate the new DBT, that it fails to capture some elements of the threat, and that the lack of a Department-wide strategy means implementation will take longer and cost more than planned. Nevertheless, witnesses pointed to tangible progress toward consolidation of nuclear material and strategies to deny even determined terrorists any access to weapons components.

But we did not hear testimony on the status of physical security enhancements at the five sites outside the active weapons complex managed by the Department's Office of Energy, Science and Environment (ESE). As the DOE National Nuclear Security Administration (NNSA) succeeds in hardening current weapons production facilities and labs, ESE sites could pose increased risk as the next tier of soft targets for terrorists following the path of least resistance.

While recent consolidation of DOE-wide security policy and oversight functions offers the prospect of consistent DBT implementation, GAO today reports ESE sites face some unique challenges keeping pace with their NNSA counterparts. Reassessment of the risk that highly enriched uranium or plutonium at ESE sites might be fabricated into an improvised nuclear device could render current security plans inadequate. Any revision to the DBT could trigger a time-consuming reassessment of all security plans. Already, the pace and cost of security strategies seem so uncertain that one site requested no funding at all for DBT implementation this fiscal year.

The good news is the stringent requirements of the new DBT appear to have transformed possession of special nuclear materials from a prestigious credential to a serious liability. Facilities now have a powerful incentive to blend down or consolidate dangerous stocks. But complex management structures, jurisdictional stovepipes and the resultant lack of clear lines of authority for key DBT-related activities create unique barriers to strengthened security at ESE sites. And answering the vexing question "How much security can we afford?" becomes even more difficult when evaluating the cost/benefit yield of capital improvements and security enhancements at decommissioned facilities DOE hopes to close sooner than later.

We are grateful for the time and expertise made available to the Subcommittee today by representatives from the Department of Energy, the General Accounting Office and the Project on Government Oversight. We particularly appreciate the patience and forbearance of our DOE witnesses who agreed to forgo their customary place on the first panel. Their forbearance and willingness to listen will allow them, and us, to engage in more meaningful and constructive dialogue.

Welcome.

Mr. SHAYS. With that, I welcome all our witnesses and now turn to the ranking member, Mr. Kucinich. I appreciate your presence here today, Mr. Kucinich.

Mr. KUCINICH. Thank you very much, Mr. Chairman. Good morning, and thank you for holding this important hearing.

Terrorist threats to all of our Nation's nuclear assets are both real and constant. According to the report of the 9/11 Commission released last week, we now know that Khalid Sheik Mohammad proposed using planes to attack 10 U.S. targets, including unidentified nuclear power plants. To think that millions of Americans could be affected by a terrorist attack at a nuclear power plant is indeed a startling and sobering notion.

It has been nearly 3 years since the tragic events of September 11. Since that time, the U.S. military has entered into Afghanistan and Iraq; the U.S. Congress created the Department of Homeland Security and the U.S. Northern Command has worked with them to coordinate homeland defense missions; security has been increased at our Nation's borders and airports; even protective barriers and security measures are being installed around this Capitol. Yet, the Department of Energy continues to lag behind the rest of the Government in its terrorism preparedness measures, especially at DOE facilities containing nuclear weapons and category I special nuclear materials, the most sensitive assets in the DOE inventory.

This is the third hearing that this subcommittee has held on the implementation of the design basis threat, which guides security measures at DOE nuclear sites, and we continue to hear the same problems over and over: Why did it take the Department 21 months to develop a new design basis threat plan and why is it taking DOE so long to implement the plan?

According to the General Accounting Office, serious improvements must be made at each of DOE's category I nuclear sites in order to meet the 2006 DBT implementation deadline. I also understand that because of concerns raised by the subcommittee and by GAO, the May 2003 DBT is currently under review again, and protection strategies and guidelines may need to be altered once more. Meanwhile, the level of protection at our Nation's nuclear sites may be inadequate.

Where is the Department's sense of urgency? The lengthy DBT review process, the lack of coordination among DOE offices, sites and contractors, and the lack of funding needed to implement the DBT is just unacceptable. While I understand that the consolidation, transportation, reinforcement, and protection of nuclear assets located at multiple sites are logistically difficult and time-consuming, we simply cannot afford any more delays.

I am hopeful that Secretary Abraham's announcements last month, that these scattered assets will be consolidated in just a few modernized and highly secure sites, and that DOE is examining ways to create elite Federal forces to provide enhanced security around them, will be in effect. This cooperation among sites, strategic thinking from Department leadership, and emphasis on efficiency must continue not just for the latest DBT plan, but also for long-term interagency projects such as the proposed nuclear waste repository.

My colleague, Congresswoman Shelley Berkley of Nevada, has introduced H.R. 2926, the Nuclear Waste Terrorist Threat Assessment and Protection Act, which would require a terrorist threat assessment of the Yucca Mountain project before it is approved. That project, as you know, involves 77,000 tons of high-level nuclear waste transported from 131 sites nationwide through 43 States in as many as 360 congressional districts for the next 30 to 40 years. Certainly, any part and parcel of that route could be a terrorist target, and it is important that DOE and Congress continue to work together to protect our nuclear assets.

And, in effect, Mr. Chairman, I would respectfully suggest that until there is an appropriate design threat basis with respect to the movement of such nuclear waste, and until there is an appropriate way of securing that waste to protect against potential terrorist attacks, that nuclear waste should not be moved. Mr. Chairman, I hope that we will finally get some clear answers to some of these problems at DOE which have left our Nation's most sensitive nuclear facilities vulnerable to terrorism.

I want to thank the Chair again for his continued leadership on this issue. Thank you.

[The prepared statement of Hon. Dennis J. Kucinich follows:]

Statement of Rep. Dennis J. Kucinich
Ranking Minority Member
U.S. House of Representatives
Subcommittee on National Security, Emerging Threats and International Relations

Hearing on "Nuclear Security: Can DOE Meet Physical Security Requirements, Part II"

June 22, 2004

Good morning and thank you, Chairman Shays, for holding this important hearing.

Terrorist threats to all of our nation's nuclear assets are both real and constant. According to the report of the 9/11 Commission released last week, we now know that Khalid Sheikh Mohammed proposed using planes to attack ten U.S. targets, including unidentified nuclear power plants. To think that millions of northeastern Ohio residents could be affected by a terrorist attack at the Davis Besse nuclear power plant is a horrific notion to me.

It's been nearly three years since the tragic events of September 11. Since that time, the U.S. military has entered into Afghanistan and Iraq. We created the Department of Homeland Security, as well as the U.S. Northern Command to coordinate homeland defense missions. Security has been increased at our nation's borders and airports. Even protective barriers and security measures are being installed around the U.S. Capitol complex.

Yet, the Department of Energy continues to lag behind the rest of the government in its terrorism preparedness measures, especially at DOE facilities containing nuclear weapons and category I special nuclear materials, the most sensitive assets in the DOE inventory.

This is the third hearing that this Subcommittee has held on the implementation of the Design Basis Threat, which guides security measures at DOE nuclear sites, and we continue to hear the same problems over and over again. Why did it take the

department 21 months to develop a new DBT plan and why is it taking DOE so long to implement the plan? According to the General Accounting Office, serious improvements must be made at each of DOE's category I nuclear sites in order to meet the 2006 DBT implementation deadline. I also understand that because of the concerns raised by the Subcommittee and by the GAO, the May 2003 DBT is currently under review again, and protection strategies and guidelines may need to be altered once more. Meanwhile, the level of protection at our nation's nuclear sites may be inadequate.

Where is the department's sense of urgency? The lengthy DBT review process, the lack of coordination among DOE offices, sites, and contractors, and the lack of funding that will be needed to implement the DBT *is all unacceptable to me.*

While I understand that the consolidation, transportation, reinforcement and protection of nuclear assets located at multiple

sites are logistically difficult and time-consuming, we simply cannot afford any more delays. I am hopeful about Secretary Abraham's announcements last month that these scattered assets will be consolidated into just a few modernized and highly secure sites, and that DOE is examining ways to create elite federal forces to provide enhanced security around them.

This cooperation among sites, strategic thinking from department leadership, and emphasis on efficiency must continue, not just for the latest DBT plan, but also for long-term interagency projects such as the proposed nuclear waste repository at Yucca Mountain.

My colleague, Congresswoman Shelley Berkley of Nevada, has introduced H.R. 2926, the Nuclear Waste Terrorist Threat Assessment and Protection Act, which would require a terrorist threat assessment of the Yucca Mountain project before it is approved. The project involves 77,000 tons of high-level nuclear

waste transported from 131 sites nationwide through 43 states and as many as 360 Congressional districts for the next 30 to 40 years. Certainly, any part and parcel of that route could be a terrorist target, and it is important that DOE and Congress continue to work together to protect our nuclear assets.

Mr. Chairman, I hope we will finally get some clear answers today to these problems at DOE, which may have left our nation's most sensitive nuclear facilities vulnerable to terrorism.

Thank you for your continued leadership on this issue, and I look forward to listening to our witnesses today.

Mr. SHAYS. I thank the gentleman.

At this time the Chair would turn to Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman. I appreciate your holding this hearing and your continued focus on the safety of our nuclear weapons complex and our nuclear material.

Last year I had the opportunity to travel with our chairman to several of our U.S. nuclear weapons storage facilities or nuclear material storage facilities, and the need for security improvements was very evident, and DOE needs to make security enhancements a priority.

One of the most troubling things in this discussion is we are not just talking about timeframes and can all of the security enhancements be done in a sufficient time. We are also discussing the issue of whether or not the design base threat, the goal, the target that we are trying to achieve has been set at a high enough mark so that we can all be confident that these facilities and these complexes will be secure.

In an issue where we have an ability to have no margin of error, it is essential that we make certain that we set a high enough target and that we diligently pursue it. I have wondered often, as we have sat through these hearings and I have participated with the chairman in the tours, as to whether or not we have been reluctant to use certain types of weapons systems to protect these facilities that at many times we have deployed for national monuments such as the Washington Monument. In looking at what is our design base threat, what we are willing to do to protect these facilities, I think we have been far too timid. And I appreciate the information that we are going to receive today from the people who have the responsibility for making certain that we keep these facilities safe.

Thank you.

Mr. SHAYS. I thank the gentleman.

At this time, I would 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. Without objection, so ordered.

At this time we would recognize our panel. We have Robin Nazzaro, Director, Natural Resources and Environment, U.S. General Accounting Office, accompanied by Jonathan Gill, Senior Analyst, Natural Resources and Environment; and also we have testimony from Danielle Brian, executive director, Project on Government Oversight [POGO].

If anyone else may be testifying, I would ask them to stand up. If it is just the two of you, as well as Ms. Brian, we will ask you to stand, raise your right hands, and I will swear you in.

[Witnesses sworn.]

Mr. SHAYS. Note for the record our witnesses have responded in the affirmative.

Before taking testimony, Ms. Watson, welcome. If you would like to make a statement, we would enjoy that.

Ms. WATSON. Thank you, Mr. Chairman. Appreciate it. I just have a few observations that I would like to share with you, and

based on the vast amount of critical assets entrusted to the Department of Energy, I am particularly concerned with the Department sites that contain nuclear material, and their vulnerability to attack. As a member that represents Los Angeles, an area of the Nation we have learned that was a potential target for the September 11 attacks, I want to assure that we are doing everything possible to protect all our nuclear facilities, not only in that area, but throughout the country. I am particularly concerned with the length of time it will take to execute the design basis threat implementation plan. Given the current security environment, it is imperative that all vulnerable sites have no security glitches. And I want to be confident that our Nation does not get harmed again by any entities that sit right in our own backyards. All facets of law enforcement, in conjunction with the Department of Energy, should be mindful of possible sites of terrorist attack and be confident that all preventative measures have been taken to protect the citizens of this country.

As we speak, I think the Director of the Homeland Security is in Los Angeles, and a few months ago, as we had a panel that laying out plans should there be a threat, I saw where they used the word "traditional." Well, what we have done traditionally is not what we should be doing now and in the future, so I hope we can come up with creative ways to address securing these facilities. Think out of the box.

So I look forward to hearing from the panel, and thank you very much, Mr. Chairman.

Mr. SHAYS. I thank you, Ms. Watson.

We will start hearing testimony. Ms. Nazzaro.

STATEMENTS OF ROBIN M. NAZZARO, DIRECTOR, NATURAL RESOURCES AND ENVIRONMENT, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY JONATHAN GILL, SENIOR ANALYST, NATURAL RESOURCES AND ENVIRONMENT; AND DANIELLE BRIAN, EXECUTIVE DIRECTOR, PROJECT ON GOVERNMENT OVERSIGHT

Ms. NAZZARO. Thank you, Mr. Chairman and members of the subcommittee. I am pleased to be here today to discuss our work on physical security at the Department of Energy's Office of Energy, Science and Environment [ESE]. ESE is comprised of nine offices, including the Offices of Environmental Management; Nuclear Energy, Science and Technology; and Science, which have sites that contain category I special nuclear material.

On April 27, 2004, we testified before this subcommittee on several key aspects surrounding DOE's development and implementation of the 2003 design basis threat. Specifically, we noted that DOE had been slow to develop DBT implementation plans and the budgets to support these plans. As a result, the Department's deadline to meet the requirements of the new DBT by the end of fiscal year 2006 was probably not realistic for some sites.

Subsequently, you asked us to examine in more detail the issues that could impede ESE's ability to fully meet the threat contained in the new DBT. After reviewing ESE's efforts to implement the May 2003 DBT at sites containing category I special nuclear material, we continue to be concerned about whether DOE can meet its

fiscal year 2006 deadline for full implementation of the DBT. ESE sites that contain category I special nuclear material have developed plans for implementing the DBT. However, we believe there are four issues that will make it difficult to implement these plans in a timely fashion.

First, ESE sites approved their implementation plans in February 2004, before the Deputy Secretary of Energy issued his guidance on which sites had improvised nuclear device vulnerabilities. ESE security officials told us that confusion exists about how or if this guidance applies to their sites. They are working with officials from DOE's Office of Security to resolve this confusion. However, the Director of DOE's Office of Security and Safety Performance Assurance agreed that additional guidance will be necessary to resolve this confusion. Consequently, the assumptions in the plans may no longer be valid and the plans may need to be revised, which could be very costly.

Second, the ESE implementation plans are based on the May 2003 DBT. As you mentioned, DOE is now reexamining that DBT and may revise it. Consequently, if the DBT is changed in a way that increases security requirements, some ESE offices may have to revise their implementation plans to reflect these changes.

Third, the plan for one ESE site is underfunded. Officials in the Office of Nuclear Energy, Science and Technology told us that for one site no DBT implementation funding had been requested for fiscal year 2005, even though the site recognized that it needed to substantially increase its protective forces to meet the new DBT.

Finally, ESE faces a number of complex organizational issues that could make DBT implementation more difficult. I will give you three examples here. For the Office of Environmental Management to fully comply with the DBT requirements in fiscal year 2006, one of its sites will have to close and de-inventory two facilities, consolidate excess materials into remaining special nuclear materials facilities, and move material, which the National Nuclear Security Administration's Office of Secure Transportation will transport to another site. Because the cost to close these facilities and to move the materials within the site are borne by the Office of Environmental Management's program budget, and not by its safeguards and security budget, obtaining adequate funding could be difficult.

At an Office of Science site, a building that contains category I special nuclear material is managed and protected by the Office of Science, while the material itself belongs to the Office of Nuclear Energy, Science and Technology. This office is currently planning to move the material and process it. After processing, the material will no longer have to meet the protection requirements for category I special nuclear material; however, accomplishing this task will require additional security measures, the planning and funding for which will have to be carefully coordinated with the Office of Science.

The Office of Nuclear Energy, Science and Technology sites face similar issues. For example, the Office of Environmental Management currently owns all of the category I special nuclear material stored at one of the Nuclear Energy, Science and Technology sites. Environmental management is currently planning to have the National Nuclear Security Administration's Office of Secure Transpor-

tation transport this material to several other locations by the end of January 2005. The Office of Nuclear Energy, Science and Technology also needs to consolidate two of its sites into a single national laboratory, which will, among other things, ensure that it has an adequate number of protective forces. If the special nuclear materials are not moved and this consolidation is not achieved, the number of protective forces at this site may not be adequate.

Because of the importance of successfully integrating multiple program activities with security requirements, we continue to believe, as we recommended in April 2004, that DOE needs to develop and implement a Department-wide, multi-year, fully resourced implementation plan for meeting the DBT requirements that includes important programmatic activities such as the closure of facilities and the transportation of special nuclear materials.

Mr. Chairman, that concludes my prepared statement. We would be happy to answer any questions you or members of the subcommittee may have.

[The prepared statement of Ms. Nazzaro follows:]

United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, June 22, 2004

NUCLEAR SECURITY

Several Issues Could Impede the Ability of DOE's Office of Energy, Science and Environment to Meet the May 2003 Design Basis Threat

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

GAO-04-894T

June 22, 2004

GAO
Accountability-Integrity-Reliability
Highlights

Highlights of GAO-04-894T, a testimony to Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

NUCLEAR SECURITY

Several Issues Could Impede the Ability of DOE's Office of Energy, Science and Environment to Meet the May 2003 Design Basis Threat

Why GAO Did This Study

A successful terrorist attack on Department of Energy (DOE) sites containing the material used in nuclear weapons, called special nuclear material, could have devastating consequences for the site and its surrounding communities. Because of these risks, DOE needs an effective safeguards and security program. A key component of an effective program is the design basis threat (DBT), a classified document that identifies, among other things, the potential size and capabilities of terrorist forces. The terrorist attacks of September 11, 2001, rendered the then-current DBT obsolete resulting in DOE issuing a new version in May 2003.

GAO examined the issues that could impede the ability of DOE's Office of Energy, Science and Environment to fully meet the threat contained in the May 2003 DBT by the department's fiscal year 2006 deadline.

What GAO Found

Five Office of Energy, Science and Environment sites contain substantial quantities of Category I special nuclear material, which consists of specified quantities of plutonium and highly enriched uranium. These sites have all developed plans for implementing the May 2003 DBT. However, there are several issues that could make it difficult to implement these plans by DOE's deadline of the end of fiscal year 2006. Specifically:

- Office of Energy, Science and Environment sites approved their DBT implementations plans in February 2004 before the Deputy Secretary of Energy issued his April 2004 guidance on which sites had improvised nuclear device vulnerabilities. As a result, some sites may be required to shift to enhanced protection strategies, which could be very costly. Consequently, the assumptions in the Office of Energy, Science and Environment DBT implementation plans may no longer be valid, and the plans may need to be revised.
- Office of Energy, Science and Environment site plans are based on the May 2003 DBT; however, DOE is now reexamining the May 2003 DBT and may revise it. Consequently, if the DBT is changed in a way that increases security requirements, some Office of Energy, Science and Environment sites may have to revise their implementation plans to reflect the need to provide for a more stringent defense.
- The plan for one Office of Energy, Science and Environment site was under funded. Specifically, officials in the Office of Nuclear Energy, Science and Technology, which is part of the Office of Energy, Science and Environment, told GAO that, for one site, no DBT implementation funding had been requested for fiscal year 2005.
- Finally, full implementation of these plans will require the successful resolution of complex organizational arrangements between various program and security offices.

Consequently, GAO continues to believe, as it recommended in April 2004, that DOE needs to develop and implement a departmentwide, multiyear, fully resourced implementation plan for meeting the new DBT requirements that includes important programmatic activities such as the closure of facilities and the transportation of special nuclear materials.

www.gao.gov/cgi-bin/getrpt?GAO-04-894T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robin M. Nazzaro at (202) 512-3841 or nazzaror@gao.gov.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our work on physical security at the Department of Energy's (DOE) Office of Energy, Science and Environment (ESE). DOE's Office of Energy, Science and Environment comprises nine offices, including the Offices of Environmental Management (EM); Nuclear Energy, Science and Technology (NE); and Science (SC) and is headed by the Under Secretary for ESE.

DOE has long recognized that a successful terrorist attack on a site containing the material used in nuclear weapons—called special nuclear material—could have devastating consequences for the site and its surrounding communities. This is particularly true at sites that contain Category I special nuclear material, which consists of specified quantities of plutonium and highly enriched uranium in the form of assembled nuclear weapons and test devices, major nuclear components, and other high-grade materials such as solutions and oxides.

Because terrorist attacks could have such devastating consequences, DOE's effective management of its safeguards and security program, which includes developing safeguards and security policies, is essential to preventing an unacceptable, adverse impact on national security.[1] For many years, DOE has employed risk-based security practices. To manage potential risks, DOE has developed a design basis threat (DBT), a classified document that identifies the potential size and capabilities of terrorist forces. DOE's DBT is based on an intelligence community assessment known as the Postulated Threat. DOE requires the contractors operating its sites to provide sufficient protective forces and equipment to defend against the threat contained in the DBT. The DBT in effect on September 11, 2001, had been DOE policy since June 1999. DOE replaced the 1999 DBT in May 2003 to better reflect the current and projected terrorist threats that resulted from the September 11 attacks.

On April 27, 2004, we testified before this Subcommittee on several key aspects surrounding DOE's development and implementation of its May 2003 DBT.[2] Specifically, we reported on our examination of (1) the reasons

[1]See U.S. General Accounting Office, *Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-04-471 (Washington, D.C.: May 30, 2003).

[2]See U.S. General Accounting Office, *Nuclear Security: DOE Must Address Significant Issues to Meet the Requirements of the New Design Basis Threat*, GAO-04-701T (Washington, D.C.: April 27, 2004).

DOE needed almost 2 years to develop a new DBT, (2) the higher threat contained in the new DBT, and (3) the remaining issues that needed to be resolved for DOE to fully defend against the threat contained in the new DBT. With regard to the issues needing resolution for DOE to fully defend against the threat contained in the new DBT, we found that DOE had been slow to resolve a number of significant issues including developing DBT implementation plans and budgets to support these plans. The need to fully resolve these issues may affect the ability of its sites to fully meet the threat contained in the new DBT in a timely fashion. Consequently, we stated that DOE's deadline to meet the requirements of the new DBT by the end of fiscal year 2006 was probably not realistic for some sites.

Subsequently, you asked us to examine in more detail the issues that could impede ESE's ability to fully meet the threat contained in the new DBT by DOE's fiscal year 2006 deadline. To carry out our objective, we interviewed DOE and ESE officials, including EM, NE, and SC headquarters security officials, as well as field security officials. We also reviewed relevant documents these officials provided to us. In addition, we reviewed recent reports from DOE's Office of Independent Oversight and Performance Assurance for the ESE sites that contain Category I special nuclear material. We also relied on our previous work on DOE physical security conducted for this Subcommittee over the last 2 years. We performed our work from May 2004 to June 2004 in accordance with generally accepted government auditing standards.

In summary, ESE sites containing Category I special nuclear material have developed plans for implementing the May 2003 DBT. However, we believe there are several issues that could make it difficult to implement these plans by DOE's deadline of the end of fiscal year 2006. These specific issues are as follows:

- ESE sites approved their implementation plans during February 2004 before the Deputy Secretary of Energy issued his April 2004 guidance on which sites had improvised nuclear device vulnerabilities. As a result, some sites may be required to shift to enhanced protection strategies, which could be very costly. Consequently, the assumptions in the ESE site plans may no longer be valid, and the plans may need to be revised.

- ESE site plans are based on the May 2003 DBT; however, DOE is now reexamining the May 2003 DBT and may revise it. Consequently, if the DBT is changed to increase security requirements, some ESE offices may have to revise their implementation plans to reflect the need for a more stringent defense.

- While ESE sites have developed implementation plans, even under the old assumptions, the plan for one site was under funded. Specifically, NE security officials told us that for one site no DBT implementation funding had been requested for fiscal year 2005.

- Finally, full implementation of these plans will require the successful resolution of complex organizational arrangements between various program and security offices.

We continue to believe, as we recommended in April 2004, that DOE needs to develop and implement a department wide multiyear, fully resourced implementation plan for meeting the new DBT requirements that includes important programmatic activities such as the closure of facilities and the transportation of special nuclear materials.[3]

Background

Five ESE sites collectively contain substantial quantities of Category I special nuclear material. These include the following:

- the Savannah River Site in Savannah River, South Carolina, and the Hanford Site in Richland, Washington, which are managed by EM;

- the Idaho National Engineering and Environmental Laboratory and the Argonne National Laboratory-West which are located in Idaho Falls, Idaho, and are managed by NE; and

- the Oak Ridge National Laboratory in Oak Ridge, Tennessee, which is managed by SC.

Contractors operate each site for ESE. The ESE program offices that oversee these sites—EM, NE, and SC—have requested about $397 million in fiscal year 2005 for security.

Two other organizations are important contributors to DOE's security program. The Office of Security in DOE's Office of Security and Safety Performance Assurance develops and promulgates orders and policies, such as the DBT, to guide the department's safeguards and security programs. The Office of Independent Oversight and Performance

[3]See U.S. General Accounting Office, *Nuclear Security: DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat*, GAO-04-623 (Washington, D.C.: April 27, 2004).

Assurance in DOE's Office of Security and Safety Performance Assurance supports the department 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.

The risks associated with Category I special nuclear materials vary but include the creation of improvised nuclear devices capable of producing a nuclear yield, theft for use in an illegal nuclear weapon, and the potential for sabotage in the form of radioactive dispersal. Because of these risks, DOE has long employed risk-based security practices. The key component of DOE's well-established, risk-based security practices is the DBT, a classified document that identifies the characteristics of the potential threats to DOE assets. The DBT traditionally has been based on a classified, multiagency intelligence community assessment of potential terrorist threats, known as the Postulated Threat. The DBT considers a variety of threats in addition to the terrorist threat. Other adversaries considered in the DBT include criminals, psychotics, disgruntled employees, violent activists, and spies. The DBT also considers the threat posed by insiders, those individuals who have authorized, unescorted access to any part of DOE facilities and programs. Insiders may operate alone or may assist an adversary group. Insiders are routinely considered to provide assistance to the terrorist groups found in the DBT. The threat from terrorist groups is generally the most demanding threat contained in the DBT.

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 most sensitive sites employ a defense-in-depth concept that includes sensors, physical barriers, hardened facilities and vaults, and heavily armed paramilitary protective forces equipped with such items as automatic weapons, night vision equipment, body armor, and chemical protective gear.

The effectiveness of the protective system is formally and regularly examined through vulnerability assessments. 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 assets, such as special nuclear material. To conduct such assessments, 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 a group of mock terrorists.

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, 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 Category I special nuclear material—and mitigate the risks to these assets to an acceptable level. Levels of risk—high, medium, and low—are assigned classified numerical values and are derived from a mathematical equation that compares a terrorist group's capabilities with the overall effectiveness of the crucial elements of the site's protective forces and systems.

Historically, DOE has striven to keep its most critical assets at a low risk level and may insist on immediate compensatory measures should a significant vulnerability develop that increases risk above the low risk level. Compensatory measures could include deploying additional protective forces or curtailing operations until the asset can be better protected. In response to a September 2000 DOE Inspector General's report recommending that DOE establish a policy on what actions are required once a high or moderate risk is identified, in September 2003, DOE's Office of Security issued a policy clarification stating that identified high risks at facilities must be formally reported to the Secretary of Energy or Deputy Secretary within 24 hours. In addition, under this policy clarification, identified high and moderate risks require corrective actions and regular reporting.

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. DOE Orders also require field offices to comprehensively survey contractors' operations for safeguards and security every year. The Office of Independent Oversight and Performance Assurance in DOE's Office of Security and Safety Assurance provides yet another check through its comprehensive inspection program. All deficiencies identified during surveys and inspections require the contractors to take corrective action.

Reflecting the post-September 11 environment, the May 2003 DBT, among other things, identified a larger terrorist threat than did the 1999 DBT. It also expanded the range of terrorist objectives to include radiological, biological, and chemical sabotage. Key features of the 2003 DBT included the following:

- *Expanded terrorist characteristics and goals.* The 2003 DBT assumes that terrorist groups are the following: well armed and equipped; trained in paramilitary and guerrilla warfare skills and small unit tactics; highly motivated; willing to kill, risk death, or commit suicide; and capable of attacking without warning. Furthermore, according to the 2003 DBT, terrorists might attack a DOE facility for a variety of goals, including the theft of a nuclear weapon, nuclear test device, or special nuclear material; radiological, chemical, or biological sabotage; and the on-site detonation of a nuclear weapon, nuclear test device, or special nuclear material that results in a significant nuclear yield. DOE refers to such a detonation as an improvised nuclear device.

- *Increased the size of the terrorist group threat.* The 2003 DBT increases the terrorist threat levels for the theft of the department's highest value assets—Category I special nuclear materials—although not in a uniform way. Previously, under the 1999 DBT, all DOE sites that possessed any type of Category I special nuclear material were required to defend against a uniform terrorist group composed of a relatively small number of individuals. Under the 2003 DBT, however, the department judged the theft of a nuclear weapon or test device to be more attractive to terrorists, and sites that have these assets are required to defend against a substantially higher number of terrorists than are other sites. For example, a DOE site that, among other things, assembles and disassembles nuclear weapons, is required to defend against a larger terrorist group. Other DOE sites, such as an EM site that stores excess plutonium, only have to defend against a smaller group of terrorists. However, the number of terrorists in the 2003 DBT is larger than the 1999 DBT number. DOE calls this a graded threat approach.

- *Mandated 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 must now implement specific protection strategies for Category I special nuclear material. In addition, sites will have to develop, for the first time, specific protection strategies for facilities, such as radioactive waste storage areas, wastewater treatment, and science laboratories, against the threat of radiological, chemical, or biological sabotage.

- *Addressed the potential for improvised nuclear device concerns.* The May 2003 DBT established a special team to report to the Secretary of Energy on each site's potential for improvised nuclear devices. Based on the team's advice, in April 2004 the Deputy Secretary of Energy designated whether a site had such a concern. This official designation was intended to help address the general dissatisfaction with previous DOE policies for improvised nuclear devices, knowledge of which was carefully controlled and not shared widely with security officials. For example, some EM sites had no information at all on their potential for this risk.

A Number of Issues May Affect the Ability of ESE Sites to Fully Meet the Threat Contained in the New DBT in a Timely Fashion

When we testified before this Subcommittee in April 2004, we stated that while DOE had issued the final DBT in May 2003, it had only recently begun to resolve a number of significant issues that could affect the ability of its sites to fully meet the threat in the new DBT in a timely fashion. These issues involved issuing additional DBT implementation guidance, developing DBT implementation plans, and developing budgets to support these plans. We noted that fully resolving all of these issues might take several years, and the total cost of meeting the new threats was currently unknown. Consequently, we stated, full DBT implementation could occur anywhere from fiscal year 2005 to fiscal year 2008, well beyond the department's goal of the end of fiscal year 2006. Because some sites would be unable to effectively counter the higher threat contained in the new DBT for up to several years, we stated that these sites should be considered to be at higher risk under the new DBT than they were under the old DBT.

After reviewing ESE's efforts to implement the May 2003 DBT at sites containing Category I special nuclear material, we continue to be concerned about whether DOE can meet its fiscal year 2006 deadline for full DBT implementation. Specifically, while ESE sites that contain Category I special nuclear material have developed plans for implementing the May 2003 DBT, as directed by the Deputy Secretary of Energy, we believe there are four issues that will make it difficult to implement these plans in a timely fashion.

First, ESE sites approved their implementation plans in February 2004 before the Deputy Secretary of Energy issued his guidance on which sites had improvised nuclear device vulnerabilities. As noted previously, the May 2003 DBT created a special team, composed of weapons designers and security specialists to report on each site's improvised nuclear device vulnerabilities. The results of this report were briefed to senior DOE officials in March 2004 and the Deputy Secretary of Energy issued

guidance, based on this report, to DOE sites in early April 2004. As a result, some sites may be required under the 2003 DBT to shift to enhanced protection strategies, which could be very costly. This special team's report may most affect ESE sites, because, in some cases, their improvised nuclear device potential had not previously been explored. In addition, ESE security officials told us that confusion exists about how or if this guidance applies to their sites, and they stated that they are working with officials from DOE's Office of Security to resolve this confusion. The Director of DOE's Office of Security and Safety Performance Assurance agreed that additional guidance will be necessary to resolve this confusion. Consequently, because ESE sites developed their plans well before this guidance was issued, the assumptions in their plans may no longer be valid and the plans may need to be revised.

Second, the ESE site implementation plans are based on the May 2003 DBT; however, DOE is now reexamining the May 2003 DBT and may revise it. In our April 2004 report, we expressed several concerns about the May 2003 DBT. In particular, we noted that some DOE sites may have improvised nuclear device concerns that, if successfully exploited by terrorists could result in a nuclear detonation. However, under the May 2003 DBT, DOE only required these sites to defend against a relatively small group of terrorists. Because we believed that DOE had not made a persuasive case for defending against a lower number of terrorists, we recommended that DOE reexamine how it applies the DBT to sites with improvised nuclear device concerns. Subsequently, in May 2004, the Secretary of Energy announced that the department would reexamine the DBT. Originally, this reexamination was to be completed by June 30, 2004. However, according to the Director of DOE's Office of Security and Safety Performance Assurance this effort will not be completed until August 6, 2004. In addition, the Director stated that the end result of this effort may only be a plan on how to revise the DBT. Consequently, if the DBT is changed in a way that increases security requirements, some ESE offices may have to revise their implementation plans to reflect the need to provide for a more stringent defense.

Third, in one case ESE does not have adequate resources. Specifically, while ESE sites have developed implementation plans, even under the old assumptions, the plan for one site was under funded. NE security officials told us that for one site no DBT implementation funding had been requested for fiscal year 2005, even though the site recognized that it needed to substantially increase its protective forces to meet the new DBT.

Finally, ESE faces a number of complex organizational issues that could make DBT implementation more difficult. Specifically:

- EM's Security Director told us that for EM to fully comply with the DBT requirements in fiscal year 2006 at one of its sites, it will have to close and de-inventory two facilities, consolidate excess materials into remaining special nuclear materials facilities, and move consolidated Category I special nuclear material, which the National Nuclear Security Administration's Office of Secure Transportation will transport, to another site. Likewise, the EM Security Director told us that to meet the DBT requirements at another site, EM will have to accelerate the closure of one facility and transfer special nuclear material to another facility on the site. Because the costs to close these facilities and to move materials within a site are borne by the EM program budget and not by the EM safeguards and security budget, obtaining adequate funding could be difficult.

- At an Office of Science site, a building that contains Category I special nuclear material is managed and protected by the Office of Science, while the material itself belongs to NE. NE is currently planning to remove the material and process it. After processing, the material will no longer have to meet the protection requirements for Category I special nuclear material. Accomplishing this task will require additional security measures, the planning and funding for which will have to be carefully coordinated between the Office of Science and NE.

- NE sites face similar issues. For example, the NE Security Director told us that EM currently owns all of the Category I special nuclear material stored at an NE site. EM is currently planning to have the National Nuclear Security Administration's Office of Secure Transportation transport this material to several other locations by the end of January 2005. According to the NE site Security Director, NE is counting on the successful removal of this special nuclear material to meet the department's fiscal year 2006 deadline for implementing the May 2003 DBT. To implement the May 2003 DBT, NE also needs to consolidate two of its sites into a single national laboratory, which will, among other things, ensure that it has an adequate number of protective forces. If the EM special nuclear materials are not moved and this consolidation is not achieved, the number of protective forces at this site may not be adequate.

Because of the importance of successfully integrating multiple program activities with security requirements, we continue to believe, as we recommended in April 2004, that DOE needs to develop and implement a departmentwide, multiyear, fully resourced implementation plan for meeting the May 2003 DBT requirements that includes important

programmatic activities such as the closure of facilities and the transportation of special nuclear materials.

Mr. Chairman, this concludes our prepared statement. We would be happy to respond to any questions that 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 and Jonathan Gill made key contributions to this testimony. Don Cowan and Preston Heard also made 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 e-mail alerts" under the "Order GAO Products" 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 [assuming Chair]. Thank you.

Ms. Brian.

Ms. BRIAN. As we prepared this testimony, it was striking to hear members of the 9/11 Commission last week come to the conclusion that no policymakers were aware that terrorists might hijack commercial aircraft and fly them into buildings. In fact, however, POGO had released to the public an internal NORAD e-mail which showed that NORAD had developed a scenario in April 2001 of a commercial airliner being hijacked and flown into the Pentagon, just 5 months before terrorists hijacked a commercial airplane and flew it into the Pentagon. This scenario was rejected at the time by the staff of the Joint Chiefs as being "unrealistic."

I feel certain that if a future devastating attack were to take place at one of the Department of Energy's nuclear weapons facilities, policymakers would again claim that no one knew that a terrorist could have attacked one of these facilities and created an improvised nuclear device, a nuclear detonation. Your hearings have been laying the groundwork to make it harder for them to make this claim.

In January 2004, DOE Secretary Abraham, Deputy Secretary McSlarrow, and Oversight Director Podonsky began a dialog with POGO regarding our recommendations for security upgrades. Since then, we have been cautiously optimistic the DOE may be turning the corner. The Secretary's May 7th speech further reassured us. This is the first time a DOE secretary has recognized and admitted the problems and the extent of the changes necessary to provide adequate security in the weapons complex.

POGO believes Secretary Abraham and Deputy Secretary McSlarrow are sincerely concerned about the state of security in the complex; however, these officials have a limited time in office.

We are not sanguine that the agenda outlined by the Secretary will become a reality. He will need to fight the weapons complex bureaucracy and its contractors, who are professionals at preserving the status quo.

And I wish I shared the optimistic of Chairman Shays when he was talking about the improvements at NNSA sites. I actually received a call last night, at about 11, from Los Alamos, where I learned that the site that we are all familiar with, TA–18 at Los Alamos, which is at the bottom of a canyon and everyone has agreed needs to be de-inventoried immediately, well, it turns out NNSA has essentially capitulated the responsibility of doing that back to the contractor at Los Alamos and waiting to hear from the contractor on their plans to move it.

One particular problem that appears to be a complex-wide phenomenon is the huge amount of overtime the guards are working. Some security officers at Y–12 are working up to 90 hour weeks. We have an internal Wackenhut document where the Y–12 security manager threatens to fire an officer whose doctor temporarily limited the officer's work schedule to only a 55 hour week after knee surgery. The security officer was forced to ask his doctor to retract this limitation or he would be fired. How can anyone claim with a straight face that people who are working 90 hours a week are alert enough to protect nuclear materials against a terrorist attack? While I know this hearing is focused specifically on Environ-

mental Management, Science and Nuclear Energy sites, I think this phenomenon of dramatically overworking the protective forces deserves the committee's immediate attention.

One disappointment of the Secretary's speech is that he did not address the security problems and lack of mission at Argonne West and Idaho National Engineering and Environmental Laboratory, the nuclear energy facilities that contain tons of highly enriched uranium and plutonium that are attractive to terrorists. There is no mission-related need for this large quantity of special nuclear materials for either of these sites. The cost of protecting these materials is huge: $40 million a year. Two years ago, when Independent Oversight tested the security at Argonne West, where the majority of this material resides, they found security unsatisfactory. In other words, the facility was unable to protect adequately the tons of highly enriched uranium and plutonium. Since then, Argonne West has had even more problems, according to sources at the site as well as in Washington.

For example, POGO has been told that Argonne West spends more money to protect the 7 to 8 tons of unneeded special nuclear material than it does on the program. However, there is a fear at the site that if DOE moves this unneeded material to a more secure location, the site might be shut down. Furthermore, POGO has been told by multiple sources that the guard force at Argonne West is 50 percent undermanned. In the last few weeks, another 10 percent of their guard force quit. Recently, Argonne West needed $1 million for quick security upgrades, but Headquarters Nuclear Energy refused them these funds. This is $1 million. It is not a lot in the DOE budget. Despite the required security upgrades after September 11, the increased DBT in spring 2003 and the Headquarters directive of April 5, 2004, to go to a denial strategy because of IND concerns, Argonne West has the same inadequate tactical response plan that they had before September 11.

Argonne West is also having serious problems developing a new site security plan; they haven't been able to develop a credible vulnerability assessment, they haven't performed computer simulations for security plans, limited scope performance tests, or full-up force on forces for several years. I recommend this subcommittee turn some of its attention directly to Argonne West. If this facility cannot protect the material, the material should be moved to a more secure location.

While similar security inadequacies exist at Idaho National Engineering Lab, there are at least plans to de-inventory the category I materials from this site by the end of 2005. The problem, however, is that the plan is to move these materials to Argonne West.

Similarly, Hanford, an environmental management site, is scheduled to be de-inventoried of all its category I materials by the end of 2005, which is a good thing, as they recently failed a force-on-force run by Independent Oversight, even after September 11 upgrades.

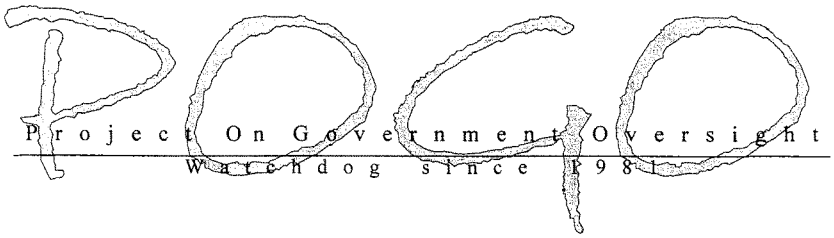
Savannah River, another EM site, stores huge quantities of plutonium. As far as we can deduce, Savannah River does not suffer from the security failures we have uncovered at these other sites, as well as at most of the NNSA sites. The ongoing problem at Savannah River, however, is a history of unfulfilled promises to build

an underground storage facility for the plutonium. Most of the plutonium at Savannah River is currently being stored in an old reactor building that was never meant to be a plutonium storage facility.

We have not developed sources at Oak Ridge National Lab, the final science site with category I materials, which stores large quantities of uranium–233, so we can't comment on their security.

Thank you again for asking me to testify and for sticking with this issue. I believe it is some of the most important work you will do in the Congress, and this subcommittee has been absolute leaders in taking on this very important job.

[The prepared statement of Ms. Brian follows:]



Testimony of Danielle Brian
Executive Director, Project On Government Oversight
before the
House Government Reform Subcommittee on
National Security and Emerging Threats on Nuclear Security:
Can DOE Meet Facility Security Requirements?
June 22, 2004

As we prepared this testimony, it was striking to hear Members of the 9/11 Commission last week come to the conclusion that no policymakers were aware that terrorists might hijack commercial aircraft and fly them into buildings. In fact, however, Project On Government Oversight (POGO) released to the public an internal NORAD email, which showed that NORAD had developed a scenario in April 2001 of a commercial airliner being hijacked and flown into the Pentagon – just five months before terrorists hijacked a commercial airplane and flew it into the Pentagon. This scenario was rejected at the time by the staff of the Joint Chiefs as being "unrealistic."

I feel certain that if an event were to take place at one of the Department of Energy's (DOE) nuclear weapons facilities, policymakers would claim that no one knew that a terrorist could have attacked one of these facilities and created an improvised nuclear device – a nuclear detonation. Your hearings have been laying the groundwork to make it harder for them to make this claim.

DOE Secretary Abraham's Initiatives

In January 2004, DOE Secretary Spencer Abraham, Deputy Secretary Kyle McSlarrow and Oversight Director Glenn Podonsky began a dialogue with POGO regarding our recommendations for security upgrades. Since then, we have been cautiously optimistic that DOE may be turning the corner. The Secretary's May 7 speech further reassured us. This is the first time a DOE Secretary has recognized and admitted the problems and the extent of the changes necessary to provide adequate security in the weapons complex.

For example, Secretary Abraham announced DOE would be reevaluating the Design Basis Threat (DBT), the security standards that facilities are required to meet. Increasing the DBT to better reflect the intelligence community's Postulated Threat is essential. This review, along with the April

666 11th Street, NW, Suite 500 • Washington, DC 20001-4542 • (202) 347-1122
Fax: (202) 347-1116 • E-mail: pogo@pogo.org • www.pogo.org
POGO is a 501(c)3 organization

5, 2004 directive requiring all sites with Improvised Nuclear Device (IND) vulnerabilities to increase their defensive posture to a "denial" strategy, will vastly improve security. An IND is an actual nuclear detonation on site, which can be accomplished within minutes by a terrorist bringing a few additional materials in a rucksack. Recently, former DOE Security Czar General Eugene Habiger stated that such a blast would be comparable to one that is one-twentieth of the Hiroshima detonation. Experts interviewed by POGO believe it would be even more devastating. In the past, the bigger concern had been to thwart the theft of nuclear materials. As a result, it was considered adequate to allow a terrorist to enter the facility but prevent him from being able to leave again. Now, the "denial" requirement means a terrorist must be prevented from entering the facility at all, given the possibility that a suicidal terrorist could detonate an Improvised Nuclear Device. Concerns about Improvised Nuclear Devices underscore the need to further consolidate Special Nuclear Materials, as a number of sites simply will not be able to meet these higher standards or afford the required upgrades.

We were pleased to hear the Secretary's plan to expedite the schedule for building the new storage facility at Y-12. Our worry is – which design? The current contractor operating Y-12, BWXT, inexplicably changed a plan to build a bermed facility covered by earth on three sides and its roof, similar to the Device Assembly Facility at the Nevada Test Site, and is now planning instead to build an above-ground facility. The change in design was approved based on the contractor's estimate that it would both increase security and save money. However, in a March 19, 2004 Inspector General (IG) report, the IG concluded that the new design for the storage facility will actually decrease security and significantly increase costs.

Another of Secretary Abraham's plans, to eliminate the burst reactor at Sandia National Laboratory and remove the highly-enriched uranium (HEU) fuel core, will save over $30 million per year in security costs by eliminating the need for extensive physical security. We are disappointed, however, in the timeline for this step. It shouldn't take three years, as this reactor currently is rarely used. For example, in early 2000 when DOE considered moving the reactor from Sandia, its next scheduled mission wasn't until October 2002, 2 ½ years later.

In addition, raising the need to blend down 100 tons of HEU is one of the highlights of the Secretary's announcement. Step one is to consolidate the materials into fewer and more secure locations. Step two is to blend down the excess HEU and immobilize the excess plutonium so that they no longer present such an attractive target to terrorists. It is important to begin working on step two.

Secretary Abraham's proposal to federalize the security forces is certainly worth considering, as it would address a number of the problems we have encountered across the complex. In the meantime, the current private security companies employing the security officers around the complex need to do a much better job in improving guard force morale by reducing overtime, increasing training, and providing adequate compensation packages.

We were also pleased to see the Department is finally going to move to a media-less computing system, which will eliminate concerns repeatedly raised by missing hard drives and computer disks.

Finally, the Secretary acknowledged that whistleblowers have been forced outside the system, often suffering retribution for telling the truth, and that there is a need for a change in the management culture. This is the third DOE Secretary I have heard say this. What can we all do to make it happen? Congress needs to pass the whistleblower protection legislation introduced by Representative Ed Markey as a first step. It is clear that Secretaries with the best intentions can not protect whistleblowers from the wrath of an angry bureaucracy.

We are not sanguine that the agenda outlined by Secretary Abraham will become a reality. He will need to fight the weapons complex bureaucracy and its contractors who are professionals at preserving the status quo. It is important that this Subcommittee obtain a timeline from DOE that will lay out milestones to accomplish these initiatives, and then hold DOE to the schedule.

One particular problem that appears to be a complex-wide phenomenon is the huge amount of overtime the protective forces are working. For example, some security officers at Y-12 are working up to 90 hour weeks. We have an internal Wackenhut document where the Y-12 security manager is threatening to fire an officer whose doctor temporarily limited the officer's work schedule to "only" a 55 hour week after knee surgery. The security officer was forced to ask his doctor to retract this limitation or he would be fired. We know from our work on security at commercial nuclear power plants that after 60 hours, fatigue sets in making any person significantly less able to perform his or her job. How can anyone claim with a straight face people working 90 hours a week are alert enough to protect nuclear materials against a terrorist attack? While I know this hearing is focusing specifically on Environmental Management, Science and Nuclear Energy sites, I believe this phenomenon of dramatically overworking the protective forces deserves the Committee's immediate attention.

DOE's Environmental Management, Nuclear Energy and Science Facilities

One disappointment of the Secretary's speech is that he did not address the security problems and lack of mission at Argonne National Lab (ANL) West and Idaho National Engineering and Environmental Laboratory (INEEL) – the Nuclear Energy and Science facilities that contain tons of highly-enriched uranium and plutonium that are attractive to terrorists. There is no mission-related need for this large quantity of Special Nuclear Materials (SNM) for either of these sites. The cost of protecting these materials is huge – $40 million a year. Two years ago, when Independent Oversight tested the security at ANL West, where the majority of this material resides, they found security unsatisfactory – in other words the facility was unable to protect adequately the tons of highly-enriched uranium and plutonium. Since then, ANL West has had even more problems, according to sources at the site and in Washington.

POGO has been told that ANL West spends more money to protect the seven to eight tons of unneeded Special Nuclear Material than it does on programs. However, there is a fear at the site that if DOE moves this unneeded material to a more secure location, the site may be shut down. Furthermore, POGO has been told by multiple sources that the guard force at ANL West is 50% undermanned. In the last few weeks, another 10% of their guard force quit. Recently, ANL West needed $1 million for quick security upgrades, but Headquarters Nuclear Energy refused them the funds. Despite the required security upgrades after 9/11, the increased DBT in Spring 2003, and the Headquarters directive of April 5, 2004, to go to a denial strategy because of IND concerns, ANL West has the same inadequate tactical response plan that they had since before 9/11.

ANL West is also having serious problems developing a new site security plan; they haven't been able to develop a credible vulnerability assessment; and they haven't performed JCATS computer simulations for security plans, limited-scope performance tests, or full-up force on forces for several years. I recommend that this Subcommittee turn some of its attention to ANL West. If the facility can't protect the material, the material should be moved to a more secure location.

While similar security inadequacies exist at Idaho National Engineering Lab, there are at least plans to deinventory the Category I Special Nuclear Materials from this site by the end of 2005. The problem, however, is that the plan is to move these materials to ANL West.

Similarly, Hanford, an Environmental Management (EM) site, is scheduled to be deinventoried of all its Category I materials by the end of 2005 – which is a good thing, as they recently failed a force-on-force run by Independent Oversight, even after 9/11 upgrades.

Savannah River, another EM site, stores huge quantities of plutonium. As far as we can deduce, Savannah River does not suffer from the security failures we have uncovered at these other sites, as well as at most of the NNSA sites. The ongoing problem at Savannah River, however, is a history of unfulfilled promises to build an underground storage facility for the plutonium. Most of the plutonium at Savannah River is currently being stored in an old reactor building that was never meant to be a plutonium storage facility.

We have not developed sources at Oak Ridge National Lab, a Science site, which stores large quantities of uranium-233, and cannot comment on its security.

POGO believes that Secretary Abraham and Deputy Secretary McSlarrow are sincerely concerned about the state of security at the nuclear weapons complex. However, these two officials have a limited time in office. The Office of Security and Safety Performance Assurance will be the entity left behind to oversee any improvements. POGO recommended in our 2001 report, U.S. Nuclear Weapons Complex: Security at Risk, that the Oversight Office be moved outside the DOE in order to establish real institutional independence. At the very least, Congress needs to formalize its communications with this Office, as it has with the Inspector General.

In the end, it is clear NO change will happen without you, the Congress, providing vigilant oversight. I believe it will be some of the most important work you will do.

Mr. TURNER. Thank you for your testimony and for your information on an issue that our chairman has been a leader in, in raising the awareness level. I also serve on the Armed Services Committee. I know that Chairman Everett, of the Strategic Forces Subcommittee, is similarly concerned, and fellow Iowan Dave Hobson, chairman of Energy and Water, has also been responding to Chairman Shays' interest in making certain that this not be an issue, as we had heard in the testimony, of money.

One of the things that concerns me, as I said in my opening statement, is we do not have the option for any margin of error here. This is something that needs to be approached with the highest level of diligence, not the minimal level of diligence. Money is not an impediment or issue; it really is an issue of what the request is. When we have a definition of what is needed, there isn't anyone who would not make certain that all resources are provided to make certain that we have the protection level that we need for these resources that could be so deadly.

Ms. Brian, as you said, one of the things that I think is most important here in these discussions is this is not theoretical. We know every day, and we can read the papers every day, that there are terrorist threats to our country and that these materials, being very deadly in their potential, would be a high value target, would be a likely target, and that our need to provide security for them should be of the greatest level of diligence. When I hear issues of the process of discussion whether a design base threat is high enough or whether or not we can meet 2006, it is very disturbing to me, because it seems to me as if this should be an issue of the design base threat being of the highest level. There shouldn't need to be a discussion of is it high enough; we shouldn't be asking do we have the capability to even get it higher. Are we constrained, either by science or technology, not to reach even higher; not do we bureaucratically believe we have taken into consideration what we need.

And for the timeframes for 2006, our threat is now. So when I traveled with Chairman Shays to a few of the facilities under the control of DOE, of course, there was the discussion of the issue of the contract forces that were guarding the facilities, whether or not they had the resources necessary, whether they were receiving the support necessary. And there were the discussions, Ms. Brian, as you had said, of whether or not some of these facilities were insufficient just in design of themselves, and that materials needed to be relocated.

But in looking at the issue of we need to do this now, the question came up, of course, of, well, what is the coordination between DOD and DOE. What do you see as the process of we have the design base threat and we are looking at how do we achieve it through 2006, but what do you see in DOE, in their efforts to say if we have a gap, if we have a need that is not being filled, where else can we get those resources now so that we are not just sitting through 2006 in a state of vulnerability?

Ms. NAZZARO. DOE did take some initial steps after September 11th, and we reported on that last year when we were here, as far as adding additional guard forces, increasing perimeter security. We think that these steps were appropriate. We would also say

that the sites are well defended right now and that they have taken some immediate steps. However, we certainly feel more can be done, and we certainly raised the concern that the design basis threat did not adequately portray the level of risk that potentially was threatening DOE facilities, particularly those that had special category I nuclear materials.

Mr. TURNER. In your answer you are talking about their internal efforts.

Ms. NAZZARO. Right.

Mr. TURNER. But in listening to the discussion that we had while we were at some of these facilities, it did seem to me as if the discussions of the design base threat or the potential for protecting the facilities was limited based upon what DOE had within its control, and that there had not been adequate thought of to what extent do we need to go outside of DOE, to what extent do we need to work in conjunction with DOD to see how we can supplement, again, with my view of we cannot have any margin of error here, and supplement what we are doing; that bureaucratic wall of within DOD versus DOE and DOD protecting the American people. But that had not been coordinated. Do you have thoughts or views on what their efforts could be to better work together?

Mr. GILL. Mr. Turner, all of the sites have a variety of memoranda of understanding and agreement with local law enforcement, FBI, FAA, and their higher level contacts as well, which I am sure DOE can talk about. But in their planning, they expect these attacks would be fast, they would be violent, and the sites would have to reply with what they have on hand. I think there are some problems with getting external responders into some of the sites because, as the subcommittee is aware, the guard force that works within the material access areas, where the special nuclear material is stored, are specially cleared and are enrolled in human reliability programs and they are very sensitive positions. So there is a real fear, for example, that a responding fire truck could be in fact a Trojan horse, that terrorists could actually use some external response as a way to gain access to the sites.

So, from our experience in talking to sites, it has been very limited. There are agreements there, but in actual attacks they probably wouldn't have time to be implemented.

Ms. BRIAN. Just to supplement that, our understanding, working with some of the special forces people who are trained in evaluating these kinds of attacks, they are usually over within 3 to 5 minutes. So we really do have to rely on the forces there to combat the terrorists.

Mr. TURNER. I appreciate your perspective. I still am concerned that there is not enough coordination and that, either onsite or external to the site, that the full options of the coordination have not been pursued. I appreciate your perspective that they are working in concert and that these attacks may occur quickly, but I do sense, whenever you begin down the process of questioning on the relationship between DOD and DOE, that there is not enough coordination. I appreciate your recognition that there is coordination and that they are working together, but I do fear that is an option that is not pursued as diligently as it could be.

Ms. BRIAN. If I might add in terms of the issue of coordination, I think perhaps a more immediate concern is the coordination between the labs and the leadership at Headquarters. I think that what you have is some real direction from Headquarters and from the Secretary's Office, and once it trickles down to the labs, it is sort of like rice pudding or something, nothing really happens.

Ms. NAZZARO. We would share Ms. Brian's concern in that regard, as far as coordination within DOE. That is certainly a first place to start. You may also want to raise the question with the DOE witnesses today. As they revisit the design basis threat, which is based on an intelligence community document, you may want to question as to what kind of coordination they are doing in developing the new DBT.

Mr. TURNER. Thank you.

Ms. Watson.

Ms. WATSON. Thank you, Mr. Chairman. That kind of dovetails right into my question.

On May 7th, the Department of Energy Secretary Spencer Abraham a series of new security initiatives. What enhancements are the DOE using now that differs from before? Enhancing these new initiatives, what is DOE doing?

Mr. GILL. We are very positive on the initiatives in that they demonstrate a commitment, leadership, and an understanding of the issues. In terms of things that are brand new, I am not sure that there is all that much that wasn't going on at some level before. Efforts such as technology department, and the various cyber security issues, those have been around for a while. Reexamining the DBT, that is something new. I think there are some things that have emerged since September 11, and primarily those have to do with protective forces. And as Ms. Brian said, they have been working extraordinarily long hours, their training has suffered, and those issues have been on the table for a while, but they now have new urgency. And having previewed Mr. Podonsky's testimony on what they plan to do with the National Training Center and related activities, I think we view that as a very positive and needed activity. But the initiatives, on the whole, are a mixture of things that have been on the table for a while, and other things that were known about for a while but have assumed new urgency since the events of September 11th.

Ms. WATSON. I was concerned by Ms. Brian's report that there are people working unbelievable hours, and to do something about that I would hope would be the first step, because as I look at homeland security, I don't look at the land, I look at the people on the land. And should they not be capable, the man who had knee surgery, it doesn't make sense, they ought to have rotating teams. So I don't know if you care to be more specific at this time, and maybe you don't have the specifics, but what are some of those changes that they are highlighting at the current time, and do they fit in with what has been reported to us?

Ms. NAZZARO. As to things that have happened since the Secretary's announcement, I would say mostly what they have done is identified what issues could impact the implementation of the DBT, what issues could impact their security, and mostly they have been studying these issues.

Ms. WATSON. Well, you know, what I am hearing is that we are kind of bogged down. You know, when you don't want to deal with something, you study it. How can we move in? I don't think we have a whole lot of time, and every time we heighten the color coded alerts, they say you need to be alert, but go on about your everyday business. Well, that is for the general public. For Government, we need to be doing something now. Post-September 11 I heard, and I am sure my colleagues did too, that they were going to use planes in buildings. Well, how ridiculous that seemed, that should have been a clue to kind of look in and see what the feasibilities are.

So I am just kind of concerned that we are studying, studying, studying, but we are not moving, moving, moving. And the people who feel that we are their enemy are planning, planning, planning, and I do feel attacks are imminent. So we have to move. We can't move with the sluggishness of bureaucracy.

I am not aiming that at you, I am just kind of relieving some of my frustration.

Ms. NAZZARO. Well, we share your concern, and one of the early concerns we had was that it took them 2 years to even develop a design basis threat after September 11th. At the hearing in April we did raise a concern that we felt that a lot of the initiatives were to develop plans, and we didn't see implementation yet. However, we also want to point out that we would like DOE to do it right. We had major concerns with the design basis threat as it was developed in May, and so we do think that this is a positive step to be revising that, but we would like to move beyond plans as well. And as Mr. Gill mentioned, we did preview Mr. Podonsky's statement, and we are concerned with the statement. They are saying that some of these initiatives would take anywhere from 90 days to a number of years.

Ms. WATSON. Well, in response—you don't even have to respond—we don't have that kind of time.

Thank you, Mr. Chairman.

Mr. TURNER. Mr. Ruppersberger.

Mr. RUPPERSBERGER. I would like to go down another avenue: the issue of the 2-years and why it took 2 years, and some of the reasons for that. And I want to focus on the area of intelligence and the fact that you feel, at this point, and one of the reasons that, I think in your report, it took 2 years was because of lack of coordination with the intelligence community.

Now, do you feel that the intelligence community has not been able to get their act together in order to help the Department of Energy as it related to the postulated threat?

Mr. GILL. We did not evaluate the quality of the intelligence or the quality of the postulated threat. We believe that was beyond our capability. What we noted was that the Department of Energy has traditionally used the postulated threat, which is a product of the intelligence community plus the security organizations of the Department of Energy, NRC, and other Government organizations, for the basis of their design basis threat. There is no question that the development of the postulated threat was delayed for a number of months, primarily for two reasons: (1) because of Afghanistan and planning for Iraq put other demands on the intelligence com-

munity, and (2) there were sharp debates among the participants in the postulated threat over terrorist capabilities. If you read the postulated threat, you will see that the sole point of disagreement in the postulated threat were the capabilities of terrorists.

Mr. RUPPERSBERGER. Let us get to the bottom line. We have a 9/11 Commission that is making a lot of recommendations right now. Whatever department you are in, wherever we are, the bottom line is national security. And it seems to me that you cannot develop a postulated threat or a plan unless you are working very closely with the intelligence community.

Now, No. 1, the intelligence community has to get their act together, and that is one of the subjects that is being dealt with right now with the 9/11 Commission and some other committees that are looking into that. But when it comes down to the issue and the threat of terrorism, you have to, in my opinion, have the intelligence community involved and giving you information, because there is also a lot of flexibility and a lot of new information that is coming.

At this point, we need to have more information and work more closely with the intelligence community in order for DOE to be able to protect the facilities from a nuclear attack? I mean, the postulated threat talks about the terrorists and identifying who they are, whether there have been thefts of certain materials, all of those different issues. I don't see how you can do one without the other. So my question what do you feel needs to be done within the intelligence community in order to get that information to DOE so that they can do what they need to do to protect our nuclear facilities. Long question, but it is important.

Mr. GILL. Yes, sir. We really are not able to address what the intelligence community needs to do; we did not look at that in detail. What I can say about it is that we believe there was a general undercurrent of dissatisfaction regarding the postulated threat within the Department of Energy. I think the subcommittee has looked at this issue as well, and there are some questions about the applicability and the quality of the postulated threat, and whether in fact that was an adequate document on which to base the design basis threat on.

Mr. RUPPERSBERGER. But from what you have seen, how can you have one without the other?

Ms. NAZZARO. Well, you can't have one without the other. And historically DOE has based its design basis threat on the postulated threat. But this year there was a difference between the two documents, and that is why we say there is a continuing disagreement, obviously, between DOE and the intelligence community as what the level of threat actually is. As to their current level of cooperation and coordination with the intelligence community, DOE might be in a better position to let you know whether they are getting cooperation.

Mr. RUPPERSBERGER. You know, one of the biggest issues right now, after September 11, is the issue of integration, is that so NSA communicates with CIA, CIA with FBI. I mean, Department of Energy needs to be at the table because of what it represents and how it deals with our national security. So I would suggest that we refocus on where we are with respect to the intelligence community

helping DOE, because it is just one component. Whether or not it is a nuclear facility or it is an office building or airplane, whatever it is, it is all national security, and I think we are getting caught up in our bureaucratic issues, and especially with DOE. I see in a report that DOE had a problem themselves of finding where they even needed to go, and it took 2 years, because of the bureaucratic debates that were going on, that they couldn't come to a conclusion themselves. Now, how they cannot come to an assessment or look at the postulated threat without getting all of the information from the intelligence community is beyond me.

Let me ask this one question. As a result of the 9/11 Commission, there is a suggestion that you have one person who oversees all of the intelligence community, and that would include the Department of Defense, all of the different areas. Do you think that by having that one person—because I notice here you have budgetary issues too—that would oversee all of budget, that would help pull all of this? Because DOE is a part of the intelligence threat because of what it represents, especially in the nuclear area. Do you have any opinion on that?

Ms. NAZZARO. We did not assess that, but I will say GAO, in general, supports coordination of efforts to avoid overlap and duplication, and so I would say in general, yes, we would agree with that statement.

Mr. RUPPERSBERGER. OK. Thank you very much.

Ms. BRIAN. Congressman, if I could just add with regards to your concerns, I would hate, however, as obviously the point that you are making, I would hate DOE to get a pass in saying that their failures are because they aren't getting good enough intelligence. I mean, I think the reality is once the intelligence came to them, they did not hit the ground running at all. And, in fact, what we find is in the beginning, in fact, the real issue, they were arguing against the DBT that was indicated by the postulated threat because they didn't want to spend that much money on it. So I think there are multiple layers of problems.

Mr. RUPPERSBERGER. I agree. There are no passes to be had. There needs to be integration on both sides of the aisle.

Ms. WATSON. Would you yield for a moment?

Another question. Tom Ridge, as I mentioned, is out in California. What role does he play in terms of looking at all the various departments, heightening the alert, and having certain things happen? I am not clear on how this all gets coordinated. My colleague just asked about intelligence. It seems to be just each department does their own thing. There has to be collaboration. So can you respond, any one of you?

Ms. NAZZARO. Well, there certainly has to be collaboration, and the Department of Energy was involved in the development of the postulated threat; they were one of the parties that helped in the formulation of that. So there is coordination and there is the collaboration of the various departments. However, as to what came out of the postulated threat, there was a disagreement; the Department of Energy did not agree with it and they did develop their own design basis threat, in accordance, which we had a problem with.

Mr. GILL. I am not sure how much the Department of Homeland Security have really added to Department of Energy Security in that DOE has had a mature security organization for years while Homeland Security is new. The single most visible and expensive impact DHS has is when DHS changes the national threat warning level. The DOE equivalent, their security condition measures, change according to the national level. So, for example, at the national current level we are at, DOE is at what they call SECON 3. They move to SECON 2, when the national level moves to orange level. It has a profound impact on DOE operations and costs them an enormous amount of money per day to implement those additional measures.

Ms. WATSON. We folded a lot of the various funding sources into and under Tom Ridge when we were formulated the Department of Homeland Security. Do you know if these various departments had their budgets cut in order to put money into Homeland Security? And to address the question that was raised a minute ago, should there be one person at the top to see that this coordination gets done? I would have thought that would have been Tom Ridge's job.

Mr. GILL. I am not sure about that one. What I can say is that the Department of Energy Safeguard and Security budget has grown substantially over the past several years, so DOE has not been losing money to Homeland Security. DOE has had real budget growth.

Ms. WATSON. But I do know that the various departments did take a portion, depending on what kind of services and tasks were put under Homeland Security. So I don't hear what the coordination is and if all these departments are talking and sharing with each other.

Ms. NAZZARO. I believe for the Department of Energy those were research capacities that were transferred to Homeland Security, it was not their security budget. Security forces were not transferred to Homeland Security.

Mr. GILL. There were some research capabilities at Lawrence Livermore National Laboratory, that are now part of Homeland Security.

Ms. WATSON. Thank you.

Mr. TURNER. Mr. Ruppersberger, actually, Ms. Watson had not exhausted her time beforehand, so if you have additional questions.

Mr. RUPPERSBERGER. No, I am fine.

Mr. TURNER. OK. Then we will go to Mr. Tierney.

Mr. TIERNEY. Thank you.

Ms. Brian, how are you? Thank you once again for coming to Newburyport, MA recently to address a group up there.

Ms. BRIAN. It is a gorgeous town.

Mr. TIERNEY. It is, thank you.

I thank the other witnesses for being here this morning.

Let me ask a question. I am looking at the GAO report and the three reasons why the Department of Energy departed from the postulated threats assessment, and I would like to go over each one and have all the witnesses speak to how reasonable they think these reasons were.

One of the reasons the officials said that they deviated was because they believe the postulated threat applied only to threats that handled completed nuclear weapons and test devices. How reasonable was it for them to have reached that conclusion, Ms. Nazzaro?

Ms. NAZZARO. We disagreed with that assessment, and what we felt was that the Department did not do an adequate job of justifying why they were differentiating between sites that had nuclear weapons and those that had nuclear materials.

Mr. TIERNEY. And did you ever get to form an opinion as to why they had made that conclusion as opposed to what I know later in your report it indicates you thought was clearly in the postulated threat?

Ms. NAZZARO. No, we have not, and we understand that is part of the reason why DOE has accepted our recommendation to revisit the design basis threat.

Mr. TIERNEY. Ms. Brian.

Ms. BRIAN. We agree with the GAO that the threat of an improvised nuclear device should really be the standard of whether a site should be reaching the highest levels of security, and not whether there is a full-up weapon there.

Mr. TIERNEY. Well, their second reason was that they believe that the higher threat levels contained in the postulated threat represented the worst potential worldwide terrorist case over a 10-year period. How were they off the mark on that and why do you think that they were off the mark?

Ms. NAZZARO. Again, we did not assess the adequacy of the DBT. What we were concerned was that they did not provide any justification as to why they were deviating from the intelligence community's input and why they came up with their own assessment. And, again, they are revisiting the DBT and I would assume that this is another issue that they are taking into consideration.

Mr. TIERNEY. I don't mean to put you on the spot, but I look at these reasons or excuses and they don't seem to be very well founded, at least the way that you have laid them out here. If we are being frank, are saying that we think they just gave us somewhat of a reason that hit them on the top of the head, that they just decided to go their own way and had no justification for why they did it other than that they found some expedience in doing that?

Ms. NAZZARO. Well, our concern was that there was no justification for these deviations other than that we understand there were serious concerns over budget, as to whether they would have enough money to be able to implement the new design basis threat. However, that has been disputed by the Department of Energy.

Ms. BRIAN. I would respond to that comment that actually these facilities represent the worst possible vulnerability, really, that is housed in the entire country, and so we would want them to be facing the worst possible threat in order to protect against that potential vulnerability.

Mr. TIERNEY. And I won't go around. I just note that the last reason they gave for it was they just didn't really think that this was anything more than a guide, a reference guide, which I think clearly is specious. I think that this committee ought to be a little concerned that the Department of Energy is throwing out those rea-

sons for not following something as serious as the postulated threat and getting to a DBT that makes some sense there.

I understand, however, the budgetary problems, and I know that at one point the Secretary submitted a rather large budget to protect some of these nuclear facilities, and the Office of Management and Budget overruled it. And I think that we ought to take a look at that also in terms of what my colleague mentioned a little earlier, as to just who is going to make these decisions on the Department of Homeland Security issues in terms of the budget. If we are not going to have one person that can override the Office of Management and Budget, how are we going to get a national security posture here that really does identify what our threats are and what our risks are, and prioritizes them and makes sure that our resources get there? And if we are going to have Department of Energy people identifying them, or at least be encouraged to identify them, they ought not to be held back by the fact that they don't think they are going to get the money or they are going to be overruled. And I think that is probably where a lot of this comes into play.

So to what extent do you as witnesses think that the budgetary concerns affected the implementation of the DBT? Do you think that was the overriding concern or do you think it was only one of several concerns?

Ms. NAZZARO. I would say we certainly think that was an overarching concern, that they looked at the extent to which they could implement the design basis threat. We feel the design basis threat should identify the threat, then DOE can decide what level of risk they are willing to take if they can't fund the whole thing.

Mr. TIERNEY. Well, it would seem to me that you at least go for all of it and what it is going to cost, and then fight like heck for the money.

Ms. NAZZARO. Correct.

Mr. TIERNEY. And then if you don't get the money, then you may have to scale back or whatever.

Ms. NAZZARO. Then you scale back and decide where you want to take risks, where you can logically take a risk, but at least accept and acknowledge that you are taking a risk.

Mr. TIERNEY. I am concerned here that there are some politics involved here, that we have only got so much money because we are running this deficit that is outrageous, and then trying to back everybody in to not complain too much and just bring themselves within those numbers, and I think that is a serious, serious danger in this country.

Ms. Brian, do you want to add something to that?

Ms. BRIAN. My one comment at the time when that happened with OMB, I think the dynamics were slightly different, and what you had was a Department of Energy that was reporting to the Congress that everything was fine, security was good, and then out of the corner of their mouth they go to OMB and say, but we need this critically important money right now. And I think they were really speaking out of two sides of their mouth at the time, and at least I think we are getting some change in that DOE is not pretending that everything is all right anymore.

Mr. TIERNEY. Thank you.

Mr. RUPPERSBERGER. Would the gentleman yield?

Mr. TIERNEY. I will yield.

Mr. RUPPERSBERGER. Just one question on this issue of budgeting. Do you have an opinion whether or not the fact that DOE was having budgetary problems because more resources are being put into homeland security and the money just isn't getting filtered back? That seems to be a pattern in a lot of departments right now. Do you have an opinion as it relates to DOE?

Ms. NAZZARO. I would have no basis to make that assessment.

Ms. BRIAN. Nor I.

Mr. RUPPERSBERGER. OK. Thank you.

Mr. TIERNEY. I yield back.

Mr. TURNER. Mr. Chairman.

Mr. SHAYS. Thank you.

Let me just run through a number of questions the subcommittee would like to have answered. This is for primarily Ms. Nazzaro or Mr. Gill, but, Ms. Brian, jump in at any time.

How optimistic are you that the ESE will make the 2006 deadline for DBT implementation?

Ms. NAZZARO. We do not feel that is realistic at this point because of a number of factors that we mentioned this morning, primarily that they are revisiting the DBT. ESE has made plans to implement the May 2003 DBT. If that DBT changes, particularly raises the level of security requirements, they will have to revise their plans. And, again, we are pushing back implementation.

Mr. SHAYS. How would you evaluate the ESE efforts to implement security criteria under the new DBT?

Ms. NAZZARO. At this point, they have developed plans, they have put money in the 2005 budget request, with the exception of one department, so they are moving forward.

Mr. SHAYS. How can ESE reduce the time it will take to implement the new DBT?

Ms. NAZZARO. Our one major concern is that they do not have a structured coordinated plan, and we think that could be a significant implementation factor given the number of organizations that are involved and need to be coordinated. So we would like to see a fully resourced, structured, strategic plan that would also include NNSA.

Mr. SHAYS. So would that be the same answer to this question: What do you think it is going to take for ESE to reach full compliance with DBT?

Ms. NAZZARO. Yes, I would say that is probably one of the primary factors.

Mr. SHAYS. Why is it important for DOE to report regularly on DBT implementation?

Ms. Brian, I would like you to respond to this as well.

Ms. NAZZARO. Well, one of our concerns certainly is whether the implementation will be fully funded, and I think the funds are going to come from the Congress. So we feel that they need to be reporting to you on the progress they are making, the adequacy of those plans, and the funds that they need to support the plan.

Ms. BRIAN. In addition, I think the fact that they have to report means it remains on the priority list of things that they are worry-

ing about, knowing they have to come back and answer to you, and I think that is why it is critically important.

I also wanted to make one point in the earlier questions you were asking. We believe there are some sites that can't ever meet the DBT and that need to be de-inventoried and closed down. I don't mean closed down, but de-inventoried of the category I materials, rather. And there is just real hostility——

Mr. SHAYS. Please give me an illustration.

Ms. BRIAN. Lawrence Livermore. They are not going to be able to, where it stands now, meet the DBT, and we believe they need to take the category I materials out of that facility. Another example is TA–18. And they were already told to do it and they still are not doing it.

Mr. SHAYS. What should be DOE's top security priority?

Ms. NAZZARO. Well, at this point, we believe that they should revisit the DBT because we want them to do it right. We don't want them to just take May DBT and say this is what we planned, and let us plan for implementation. We want to make sure that what they are putting in place is the right plan. But we also believe that once they have that plan in place, that there needs to be a department-wide fully resourced coordinated plan.

Ms. BRIAN. I can give you three top priorities. They need to move the materials at Oak Ridge to a bermed underground facility, they need to de-inventory TA–18, and get the materials out of Lawrence Livermore.

Mr. SHAYS. How would you evaluate ESE's organizational structure?

Ms. NAZZARO. Right now, as far as the category I special nuclear materials, there is a lot of confusion. We have sites where the site is managed by one entity within the organization and yet there are materials that are owned by another entity. As Ms. Brian mentioned, one of the strategies that we have proposed in the past is to consolidate materials, move materials to other sites. That is going to require the Office of Secure Transportation. So there certainly are some problems with implementation. The other issue is that they still don't all know who the DBT is going to affect; there is still a lot of confusion as to the Deputy Secretary's memo as to who it applies to.

Ms. BRIAN. I think the biggest problem is there isn't a will at the site level. I think someone needs to go down there and pick these people up by their shirt collars and shake them and tell them to do it tomorrow, or yesterday, frankly.

Mr. SHAYS. I would like the professional staff to now ask a question.

Mr. CHASE. Ms. Nazzaro, one of the issues that GAO raised was the issue of problems with ESE's organizational structure. Were you referring to issues dealing with a centralized security office? And if you were, can you expand on that?

Ms. NAZZARO. We did not make a recommendation, but as we were going through the last couple months, when you asked us to look at ESE, that certainly came to mind as an option, that because of the convoluted organization, particularly with regard to the category I special nuclear materials. It seemed like that would

be a prudent structure, to have a centralized security force comparable to NNSA's security force.

Mr. CHASE. Did you have a discussion with ESE about that?

Mr. GILL. We have not directly discussed that issue with ESE. We have talked with senior members in the Department, senior officials in the Department that have indicated that is a possibility. There have been some planning efforts to do diagrams of, say, like a matrixed security organization for the entire ESE family of program offices.

Ms. BRIAN. I am not sure there is really even a reason to have a distinction between the NNSA sites and the ESE sites, I think there should be a centralized security within the system. And we also have been advocating for a long time that independent oversight function outside the Department and be able to be checking on how it is going on inside the system.

Mr. SHAYS. Let me ask regarding improvised nuclear devices, I will refer to them as INDs. Why did DOE issue IND vulnerability guidelines after the new DBT was released?

Mr. GILL. The guidelines for INDs are actually part of the May 2003 DBT. A special annex in the 2003 DBT established a team to go out and look at sites IND vulnerabilities. That team took some time to meet, gather data and analyze that data, and issued their report in April 2004. It was a several month period that they did this investigation.

Ms. BRIAN. I would add that I don't think we would be talking about INDs today if this subcommittee wasn't taking the leadership in starting to require people to address the concerns,

Mr. SHAYS. How will the addition of IND guidelines affect DBT implementation plans?

Ms. NAZZARO. Well, at this point there is still not total clarity as to what those guidelines mean. Some of the sites still don't feel that they know whether the DBT applies to them or not, and so that is going to impact the development of their plans and the ultimate implementation of the DBT. Even the Office of Oversight has said that further guidance is needed.

Mr. SHAYS. Let me just ask this question. What is the root cause for the security issues raised by the recent inspections of Argonne National Lab West and Idaho National Engineering and Environmental Laboratory sites?

Mr. GILL. Mr. Chairman, Argonne West, if you go by the OA inspection reports, which they had three in as many years, has shifted responsibility from a variety of program offices. There is currently not a Federal safeguard and security manager at that site; it is managed by the University of Chicago, where across the street INEEL is managed by a division of BWXT and has an onsite Federal safeguards and security manager. So even though the two sites are immediately adjacent to each other, they are managed as two different sites. The solution to that, and the Department of Energy has actually put that into motion now, is to consolidate those two facilities under a single contract with a single contractor into the Idaho National Laboratory. And then, too, that would firmly be a part of NE, Nuclear Energy Science and Technology. When they can consolidate that, that will provide a solution to some of their issues, their primary issues for security.

Mr. SHAYS. I would be interested to know, Ms. Nazzaro, what statements Ms. Brian has made that you might take issue with or qualify. During the course of her responding to questions, was there anything she said that you would have taken issue with or just want to qualify?

Ms. NAZZARO. Probably the only thing that comes to mind, because we certainly agree that DOE needs to take some action with consolidating materials, possibly even moving them from some sites, even consolidating within sites, one area that we don't see problematic right now is Mr. Podonsky's shop. Regarding the recommendation that be moved outside of DOE, we don't see a concern as far as independence or a lack thereof.

Ms. BRIAN. If I could just elaborate on my point there. That has been a longstanding concern of ours, not because of the work of that office currently. My concern is that Mr. Podonsky is not always going to be the head of that office and Secretary Abraham is not always going to be the Secretary of that office. So at the moment I don't think we do have the problems that we saw in the past from that office and that I am afraid we are going to see in the future. Right now I think it is working very well, but I am worried about when you have independent oversight, but they are not really independent, they are right inside working for the Secretary.

Mr. SHAYS. Well, is your comment basically, given the existing personnel, it works, but you are not sure under different personnel it might not work as well? Is that your point?

Ms. BRIAN. Well, when you look structurally at how it is set up, it is really not independent; I mean, the budget is based on the Secretary's discretion. That is right. And historically it hasn't worked as well.

Mr. SHAYS. So the answer is yes. In other words, it is working now only because you have confidence in the people.

Ms. BRIAN. That is right.

Mr. SHAYS. OK.

Thank you, Mr. Chairman.

Mr. TURNER. Thank you.

Mr. Duncan.

Mr. DUNCAN. Thank you, Mr. Chairman. I certainly appreciate yours and Chairman Shays' hard work on this very important issue in calling these series of hearings.

Chairman Shays said in his opening statement—I was at another hearing, so I did not get to hear it, but he says, in answering the vexing question how much security can we afford becomes even more difficult when evaluating the cost-benefit yield of capital improvements and security enhancements, and he is talking about decommissioned facilities, but it made me think back to a comment that came a few days after the original September 11 tragedies. I was eating out with former Congressman Sonny Callahan and several other Members, and Congressman Callahan was a senior member of the Appropriations Committee, and he said that he estimated we would spend a trillion and a half dollars over the next 5 years on security measures that we wouldn't otherwise have done. And nobody really challenged him, including me, but I thought at the time that was awfully high. But since then I have begun to wonder, because just a few weeks ago Federal Express,

just one company, I know they are a big company, but they told me they had spent $200 million since September 11 on security improvements. And when you start thinking about all that the Federal Government has spent, all that the State governments, the city governments, county governments, all the private companies, I mean, it has just got to be a mind-boggling figure.

And I assume that none of you have a figure on exactly how much we have spent on security in the almost 3 years since September 11 at these five facilities, but I would appreciate it if you would get those figures for me, if you would ask those facilities how much they have spent on security enhancements and improvements since that September 11 incident, at the five facilities that we are emphasizing in this hearing. If I am wrong, if somebody has those figures, now—do any of you have those figures?

Ms. NAZZARO. The only number we have is what is in the fiscal year 2005 budget for ESE; they are asking for $397 million.

Mr. DUNCAN. Well, that wouldn't be what I am asking.

Ms. NAZZARO. Are you asking for money spent since September 11th.

Mr. DUNCAN. You know, former Governor Gilmore, who chaired the Commission on Terrorism, on the threat and what to do about it, after extensive investigation into the threat, he sent a cover letter on the report, a cover letter to the President, and he said there will never be a 100 percent guarantee of security for our people, the economy and our society. We must resist the urge to seek total security; it is not achievable and drains our attention from those things that can be accomplished. And I remember reading a few months ago, in the National Journal magazine, and I think almost anyone familiar with that magazine would say it is one of the most nonpartisan publications that you could come up with, and they said in this article that we are many thousands of times more likely to be killed by a car wreck or cancer or a heart attack than we are to be killed by a terrorist event, and that we are more likely to be struck by lightening than killed by a terrorist.

And I am not saying that we shouldn't do anything about it; we need to do as much as we possibly can, especially at nuclear facilities. On the other hand, at the Federal level, we always have a tendency to overreact to any problem because every agency or department always wants more money, and so they shout very loudly about the problem they are dealing with and the contractors that deal with that department or agency always put pressure on for more money. And yet I remember the Wall Street Journal had an editorial after we passed the farm bill, and they said it was ridiculous that we had renamed it the Farm Security Act, and they pointed out that almost every department and agency in the Federal Government was using the threat of terrorism and the word security as a means of getting more money for whatever department or agency.

All I am saying is this, I go back to what the chairman said, the vexing question of how we evaluate the cost-benefit yield and so forth. And it is a difficult question. I remember hearing on NPR News one morning a few months after September 11, and they said the new Department of Homeland Security, which was just a few months old at that time, already had some figure like 3,782 devices

or security-type measures; and I know going through those must have been an extremely difficult job.

But how do we achieve that balance? You know, Government has to do many other things besides fight terrorist or the security threat, and I am assuming that while things can always be better and you always can do more and you always need to seek improvements, I am assuming that security is much better and much improved in the almost 3 years since September 11. Ms. Brian might not, but would all of you agree that we have gotten a little something for all the money that we have spent and all the time and attention that has been devoted to it? I mean, I would be shocked if you would tell me that security is not much better now than it was at the time of September 11.

Ms. NAZZARO. I would say it is not even across the DOE sites. DOE did take immediate steps after September 11th, and as security levels changed from red, yellow, orange, DOE has reacted appropriately and changed their SECON levels, which brought on more guard forces and changed the access to the facilities. Our concern is that, with the current DBT, we feel that they have not identified really what the risks could be. What we would like to see is that they develop a DBT that accurately portrays the risk and then they make a determination of changes needed. If it's funding constraints or whatever the constraints may be, that should be identified. It may be the technology isn't there.

Mr. DUNCAN. Well, you are not really answering exactly what I asked. You are giving a good answer, but what I am asking is are you telling me that none of these five facilities that we are emphasizing, are you telling me they haven't greatly increased security since September 11, 2001? Because when I go out and visit Oak Ridge, which is not in my district, but which is just a few miles, half the people that work at Oak Ridge live in my district, and they tell me all kinds of things that they have done in regard to security since September 11 to greatly increase it. And you are sitting here telling me that these facilities have not greatly increased security?

Mr. GILL. Mr. Duncan, at any DOE site, there are more guns, guards, and gates there than there were prior to September 11. There has been more money spent and DOE, for example, in fiscal year 2005, they will spend well over $1 billion on security out of a $21 billion budget. The Department of Energy has increased its security measures, but there have been some negative aspects of those too, and primarily, as people have talked about today, in terms of protective force overtime, and lack of training. But whereas DOE sites have increased their measures, how do those measures help mitigate a greatly increased design basis threat. At some places they might be able to meet the threat today; at other places it is either unknown or they have a considerable way left to go.

Mr. DUNCAN. Well, I will say this. It is not just a bunch of untrained guards that have increased security, I mean, all the people at the highest levels. I know this is true at Oak Ridge. Now, honestly, I don't know about these other facilities, but I would be greatly surprised if it is not the same at these other facilities. The leaders at those facilities have spent a lot of time and given a lot of attention to security-related matters since September 11, 2001,

and those are some of our most brilliant people that we have in the country.

Mr. GILL. I share that feeling with you, that as we visited sites and we went to 10 different places over a couple of years, including Y–12, twice, we never had any question about peoples commitment. We believed that people were doing as good a job as they could with the resources they had.

Mr. DUNCAN. Let me ask one last question, since I was interested in the money and you did come up with this figure of a little over $1 billion out of the $21 billion. What would have been that comparable figure if you had been asked that question at a hearing prior to September 11, 2001? Are we spending twice what we were then, three times, four times? Do you have any kind of estimate?

Mr. GILL. I don't, and I would have to defer to DOE for those exact numbers. The funding has increased. NNSA's safeguard security funding, for example, has gone, over the past couple of years, from about $500 million a year to over $700 million. ESE's has been a little bit different because they have been in the process of closing some facilities. I don't have an exact number on hand, but especially within NNSA it has been substantial.

Mr. DUNCAN. And those have been years of 2 to 3 percent inflation, too, so a lot of the agencies have not received huge increases.

Thank you very much, Mr. Chairman.

Mrs. BRIAN. Congressman, if I could just respond to the concerns you had about funding, Mr. Duncan. Actually, our recommendations would be saving money rather than costing more money; that often spending money on security is money down the drain, and that by consolidating the number of facilities that you have to protect at the highest levels, you don't have to have that many facilities across the country, reduce the number of facilities. Those that remain open without category I materials would dramatically reduce the funding need for security in the future.

Mr. TURNER. Thank you.

Before we close this panel, I will ask if any member of the panel has anything else they would like to add in closing. If not, then we thank you for your testimony today, and we will turn to panel two, which will include David Garman, Under Secretary, Office of Energy, Science and Environment, Department of Energy; and Glen Podonsky, Director, Office of Security and Safety Performance Assurance, Department of Energy.

Gentlemen. In this committee we do swear in our witnesses, so I would ask you if you would stand and raise your right hands.

[Witnesses sworn.]

Mr. TURNER. Please note for the record that the witnesses responded in the affirmative, and we also note that several members of your staff who are present who might be called on by you to add additional information did stand and take the oath.

We will start with Mr. Garman.

STATEMENTS OF DAVID GARMAN, UNDER SECRETARY, OFFICE OF ENERGY, SCIENCE AND ENVIRONMENT, DEPARTMENT OF ENERGY; AND GLENN S. PODONSKY, DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSURANCE, DEPARTMENT OF ENERGY

Mr. GARMAN. Thank you. I would like to thank the chairman, the subcommittee, and the General Accounting Office for their attention to the subject of this hearing. We welcome this oversight; it adds tremendous value to our efforts to ensure that we are taking the security of our sites as seriously as possible, and, to put it bluntly, this is an area where failure is not an option. And, at the same time, I agree with what has been said here this morning, we are not yet where we need to be with respect to security. So, again, Mr. Chairman, to you, your staff, and to the General Accounting Office, our thanks.

Of course, in the time since this subcommittee held its last hearing on this matter, Secretary Abraham announced 14 security initiatives to further enhance security across the DOE complex. These initiatives are detailed in the testimony submitted by Mr. Podonsky, so I need not comment on them further other than to say that NNSA, ESE, and the Office of Security and Safety Assurance are working diligently to implement them. It is safe to say that at no time has security been taken as seriously at DOE as it is being taken today and, given the events of September 11, that is as it must be.

In a prior hearing you heard from the Director of NNSA, so I will focus on the sites managed by the rest of the Department, which we refer to as Energy, Science and the Environment [ESE]. As you know, we have category I quantities of special nuclear material at five of the ESE sites under my line management authority: Hanford, the two sites in Idaho, Oak Ridge, and Savannah River. While the category I special nuclear material at each of these sites is securely housed in robust storage facilities, we are continuing our efforts to further consolidate or eliminate that material.

Turning now to the specific recommendations in the GAO report. The first recommendation involved evaluating the cost and effectiveness of existing security conditions. Every ESE site has been operating at an enhanced level of security since September 11, and at the time GAO was collecting data for its report, we had not yet analyzed the added benefits of the security enhancements implemented under the various security conditions [SECON] levels. Since that time, we have conducted vulnerability assessments at the five ESE sites possessing Cat I special nuclear materials and found that the enhanced security measures do provide additional security against covert introduction of large vehicle bombs and other infiltration into the site. However, we continue to refine our manpower-intensive approaches to security.

The second, third, and fourth GAO recommendations involved the re-examination of the May 2003 design basis threat. As has been mentioned this morning, on May 6, 2004, the Deputy Secretary directed that such re-examination be undertaken with particular emphasis on the GAO recommendations. ESE is actively and fully participating in this effort, and Mr. Podonsky's testimony provides further details on that point.

The fifth and sixth GAO recommendations pertain to the implementation of the 2003 design basis threat. We have now prepared implementation plans for each of the ESE sites possessing category I special nuclear material. These plans have been reviewed and approved by the respective program offices; they are currently under review in the Office of Security. These are aggressive plans designed to bring all sites into compliance with the May 2003 DBT by the end of fiscal year 2006. This will be a challenge, but that remains our goal. Fiscal year 2004 and 2005 funding has been identified, and it is our intent that the fiscal year 2006 budget we will propose to OMB will be sufficient to complete all necessary actions by the end of fiscal year 2006.

The Deputy Secretary's classified memorandum of April 5, 2004, did direct a change in protection strategy for some storage locations at some of our facilities, and I know that is a matter of concern to GAO. Vulnerability analyses are still underway that will likely require us to make some adjustments. Nevertheless, the Secretary's goal that we fully implement the DBT by the end of fiscal year 2006 remains in place.

You might ask is this a moving target, and how will we chase it? I would respond that this is an iterative and continuing process. I know the Secretary, the Deputy Secretary, the NNSA Director and I, as long as I serve as Acting Under Secretary, will remain engaged in this issue, which leads me to the final GAO recommendation concerning quarterly reporting, corrective actions, and the identification of high risk sites. I will assure you that I will personally review the quarterly reports, and will take actions to ensure that we are making progress against our goals.

With that, Mr. Chairman, I will stop and welcome any questions you might have either now or in the future. I am mindful of the fact that this is not a single hearing, but a process of continuing oversight, so I will look forward to working with you, the subcommittee and staff in the future.

Thank you.

[The prepared statement of Mr. Garman follows:]

STATEMENT OF

DAVID GARMAN

ACTING UNDER SECRETARY, ENERGY, SCIENCE AND ENVIRONMENT

DEPARTMENT OF ENERGY

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

June 22, 2004

Unclassified Congressional Testimony
Subcommittee on National Security, Emerging Threats, and International Relations
House Committee on Government Reform
June 22, 2004

Introductory Remarks

Mr. Chairman and members of the subcommittee, I want to thank you for inviting me to testify today regarding implementation of the Department of Energy's May 2003 Design Basis Threat at Energy, Science, and Environment sites. Our primary roles and missions include pursuing basic and applied science in the nation's interest, remediating the environmental legacy left us by weapons production and other national security pursuits during the Cold War era, protecting the nation's environmental quality, ensuring that current Department of Energy operations do not create unnecessary hazards to the health and safety of our workers and the public, and ensuring that the unavoidable hazards we must accept are mitigated by effective environmental, safety, and health programs. Let me emphasize, however, that although we at Energy, Science, and Environment have these important responsibilities in areas of national priority, we do not take our security responsibilities lightly. We understand that our operations must be conducted safely and securely. We are fully aware of the challenges presented by the current threat environment and the considerable potential risk to our facilities, assets, and personnel. Everyone in Energy, Science, and Environment having security responsibilities – from myself to our individual employees – is aware that we live in dangerous times and that we have custody of particularly sensitive information, materials, and facilities that must be protected from a range of potential adversaries. The Secretary, Deputy Secretary, and I are committed to meeting our protection

challenges and we have provided the impetus for numerous improvements in our protection programs, some of which I will discuss in this testimony.

The Subcommittee has asked that we specifically address Energy, Science, and Environment processes for developing and evaluating the 2003 Design Basis Threat implementation plans, the status of implementation efforts at Energy, Science, and Environment sites containing Category I quantities of special nuclear material, and cost estimates for complete implementation of the Design Basis Threat at these facilities. The Subcommittee has asked that I focus on these three specific issues as they relate to the General Accounting Office's report: *Nuclear Security: DOE Needs To Resolve Significant Issues Before It Fully Meets the New Design Basis Threat.*

Let me begin by reminding you that Energy, Science and Environment has four sites with Category I quantities of special nuclear material: the Hanford site near Richland, Washington; Idaho National Engineering and Environmental Laboratory; Oak Ridge National Laboratory in Tennessee; and the Savannah River Site in South Carolina. The Category I special nuclear materials at each of these sites are located in robust storage facilities; however, we continue to actively seek effective and efficient ways to further consolidate and protect that material. For example, at Hanford, by 2007 we plan to have Category I material either be moved to another storage site at Hanford or, preferably, transported to a long term storage site elsewhere. At Oak Ridge National Laboratory, we currently plan to begin processing and down blending special nuclear material in 2007, and to have all Category I material removed by 2011. Our Office of Nuclear Energy, Science, and Technology is investigating the possibility of starting this down blending effort in 2006, which would provide a commensurate earlier completion date.

Let me address the GAO recommendations, in turn, with specific reference to these four sites. The first recommendation involved evaluating the cost and effectiveness of existing security conditions (SECONS) implemented at ESE sites in conformance with *DOE Notice 473.8 Security Conditions*. Every DOE site, including ESE sites, has been operating at an enhanced level of security readiness since 9/11. The DOE Notice mandates implementation of specific security enhancements associated with each DOE SECON level. SECON levels, in turn, reflect the current national threat advisory level set by the Department of Homeland Security as well as any specific threat information associated with a particular DOE site. The actual site response to a given SECON level is dictated by an approved SECON plan for that site. At the time GAO was collecting data for the referenced report, ESE sites had not yet specifically analyzed the added benefits of the security enhancements implemented under the various SECON levels. Since that time, ESE sites possessing Category I special nuclear materials have conducted additional vulnerability assessments that explicitly examined the enhancements associated with the SECON level that has become routine over the past three years – SECON 3. In general, the results indicate that the enhanced security measures associated with SECON 3 provide additional security against certain types of adversary actions, such as adversary infiltration of the site and covert introduction of large vehicle bombs onto the site. As we have studied the implementation of these enhanced protection measures at our sites over the past three years, we have identified a number of approaches to refine the initial, manpower intensive responses that we made immediately following 9/11. We continue to identify opportunities to increase the effectiveness and efficiency of enhanced security measures by enhancing access control, barrier, detection, and

assessment technologies with respect to manpower-intensive measures such as stationing additional protective force members to examine every badge as individuals make routine entry.

The second, third, and fourth GAO recommendations involved a reexamination of the May 2003 Design Basis Threat. Specifically, they addressed the approach used to develop the revised DBT, the approach used to address improvised nuclear devices, and the appropriateness of the protection criteria used for radiological, biological, and chemical sabotage. On May 6, 2004, the Deputy Secretary directed the National Nuclear Security Administration (NNSA) and the Office of Security and Safety Performance Assurance (SSA) to review the 2003 Design Basis Threat, with particular emphasis on the GAO recommendations, to determine whether changes are needed. ESE will actively participate in this reexamination effort and I will personally monitor this effort to satisfy myself that it produces a Design Basis Threat based on documented analyses of the best available intelligence information. I feel confident that this effort will be fully responsive to the GAO concerns, and I assure you that ESE will support and implement any requirements that may result. I understand that Mr. Podonsky, the SSA Director who is also to testify today, will have further details for you concerning that review.

The fifth and sixth GAO recommendations involved implementation of the requirements of the 2003 DBT. Implementation plans have been prepared for each of our ESE sites possessing Category I quantities of special nuclear material. These plans have been reviewed and approved by the respective program offices, and they currently are being examined by the Office of Security. As the GAO report points out, these plans include very aggressive completion schedules to allow all sites to be in compliance with the May 2003 DBT by the end of FY 2006.

We have already identified funding to support these plans in FY 2004 and FY 2005, and we are now preparing our FY 2006 budget, which will reflect the funding needed to complete all necessary actions by the end of FY 2006. Of course, these plans are based in part on some key assumptions and upon studies and analyses that are not yet complete. For example, the current goal at Hanford is to remove all Category I and II special nuclear material from K-Basin, the Fast Flux Test Facility, and the Plutonium Finishing Plant by the end of FY 2006. The material to be removed from K-Basin and the Fast Flux Test Facility is planned to be processed on-site to prepare it for long-term storage and disposal. Some of the special nuclear material currently stored at the Plutonium Finishing Plant will either be moved to another storage site at Hanford or, preferably, transported to a long term storage site elsewhere. At the Savannah River Site, the implementation plan envisions further consolidation of special nuclear material on-site in some cases, and, in other cases, limited processing of the material to enable concentration of Category I and II special nuclear materials into those storage facilities that are most robust to resist incursions. At Oak Ridge National Laboratory, we are taking advantage of technical support offered by the Office of Security to identify cost-effective security measures that can support the limited processing effort required to down-blend and relocate the special nuclear material in our remaining Category I facility at that site. I believe that the assistance provided by the Office of Security will allow us to apply innovation and technology to achieve our operational and security goals, rather than just relying on manpower intensive protective force solutions. This is especially important at a site like this, where enhanced security measures will be required only for a limited time preceding the decommissioning of the facility. So, while our implementation plans are based on the best currently available information and projections, we understand that we must remain alert to conditions that may affect those plans, and we must maintain the

flexibility to implement any modifications to the plans that may be necessary to ensure that we meet our established implementation goals.

A new factor that will have some impact upon the level of protection at some ESE sites is the classified April 5, 2004, memorandum from the Deputy Secretary entitled, "*Results of the Design Basis Threat Annex Special Evaluation Team*." This memorandum directed a change of protection strategy for some storage locations at some of our facilities. Our sites that are affected by this requirement are conducting vulnerability analyses to fully analyze its implications, but the final results, including the impact on funding projections, are not yet available. However, the Department remains committed to our goal of fully implementing the May 2003 DBT by the end of FY 2006, and will work to incorporate changes dictated by this new requirement into ESE implementation plans.

The final GAO recommendation concerns the required quarterly DBT implementation plan status reports required by the Deputy Secretary and the identification of any ESE facilities that are currently considered to be at high risk under the new DBT. With regard to the quarterly reports, I will be receiving those as required from my program offices, as will the Office of Security. I can assure you that should any of those reports reflect any significant deviations from critical milestones, I will immediately take actions necessary to address those deviations. I will also rely on the Office of Security to review those reports and to advise me of any potential concerns that they may identify. Mr. Podonsky has assured me that he is prepared to offer any technical assistance we may require to keep these projects on track.

With regard to high-risk facilities, no ESE facility is currently considered to be at high risk under the new DBT. While we have identified a number of permanent security enhancements that we will work to implement, we have already applied compensatory measures where necessary to maintain acceptable levels of risk until those permanent enhancements are complete.

I now want to depart somewhat from the specifics of the GAO report to provide a more comprehensive overview of our strategy for improving security at ESE sites. In his speech on May 7, 2004, Secretary Abraham announced 14 security initiatives. I want to focus especially on some of them that are closely aligned with ESE strategic objectives – consolidation of special nuclear materials, increased use of security technologies, and the initiatives concerning cyber security.

Consolidation of special nuclear materials is a keystone of ESE's overall mission, as well as of our plans to implement the new DBT. The Office of Environmental Management, in their role of managing the accelerated cleanup of sites no longer needed by the Department, is focused upon the removal of all special nuclear materials from a number of facilities, including the Hanford Site K-reactor basins, Fast Flux Test Facility, and Plutonium Finishing Plant, and the F-Canyon and FB-Line at the Savannah River Site. We have already successfully demonstrated our ability to consolidate materials at the Rocky Flats Environmental Technology Site in Colorado and at other sites. In fact, ESE has led the way and has been the backbone of material consolidation in DOE. We need to do more, of course. For example, we must continuously examine our programs to ensure that we do not continue to store special nuclear materials in quantities exceeding mission needs. I assure you that I will continue to focus on identifying opportunities

to further consolidate special nuclear materials at our sites and to reduce the number of Category I and II storage sites.

I share Secretary Abraham's belief that we can improve the effectiveness and efficiency of our protection systems through the intelligent application of security technologies that provide force multipliers for our protective forces and reduce our reliance on manpower-intensive solutions to protection requirements. I previously mentioned our current efforts to do just that with our project at Oak Ridge National Laboratory involving the assistance and cooperation of the Office of Security. I support the Secretary's security technology initiative, and ESE intends to mine the results of the Blue Sky Commission's efforts and the results of other technology development efforts to select technologies that are appropriate for the protection systems at our sites.

The Secretary announced three initiatives aimed at improving the Department's cyber security posture: expanded cyber security performance testing by SSA's Office of Independent Oversight and Performance Assurance; various enhancements in cyber security policy, network intrusion detection systems, and dissemination of critical cyber threat information; and a technology initiative aimed at developing diskless workstation technology to a level that can support the most intensive scientific calculations. I am excited about these initiatives. Cyber technology is at the core of much that we do at ESE. I am pleased to tell you that we had made strides in some of these areas even before the Secretary announced his broader initiatives. In particular, we have been working with the Office of Independent Oversight and Performance Assurance for almost a year in a program involving enhanced cyber security testing of Office of Science facilities. We have had very positive results from this effort and have identified and corrected a number of

potential vulnerabilities in our unclassified cyber systems. This effort is ongoing and we continue to profit by it. We look forward to better communications and refined and clearer policy that supports more effective identification and implementation of cyber security programs at our laboratories and other facilities. Finally, we recognize the importance and security benefits of establishing diskless environments for our classified networks, as appropriate technology becomes available. Overall, we are supportive and enthusiastic participants in the Secretary's cyber security initiatives, and will continue to push forward in this area.

In conclusion, I want to assure you, Mr. Chairman and Members of the Subcommittee, that my colleagues and I at ESE are fully aware of the tremendous responsibility we have for protecting the special nuclear materials, information, and other national security assets residing at our facilities. Since 9/11 we have worked to improve the robustness and effectiveness of our protection programs, and we believe we are successfully meeting the challenges associated with implementing the new DBT. However, I also want to assure you that we fully understand that we cannot rest on our laurels or be satisfied with our recent accomplishments. I intend to maintain the focus on DBT implementation and to emphasize the need to effectively capitalize on the fruits of the Secretary's recent security initiatives. We have made substantial progress, but we cannot afford to rest now. I am committed to ensuring a strong and effective protection program throughout ESE, and I will work with the Department's other senior managers to ensure that we continue to strengthen what I believe is already a good program.

Thank you. This concludes my prepared testimony.

Mr. TURNER. Thank you.

Mr. Podonsky.

Mr. PODONSKY. Thank you, Mr. Chairman and members of the subcommittee. I too want to echo Mr. Garman's thanks for holding this hearing on this very important subject, and also thank you for inviting me to testify once again.

Since my last appearance before you on April 27, the Secretary has announced 14 security initiatives. These are initiatives that are tangible expressions of the Secretary's commitment to the security of the special nuclear material and other national security assets entrusted to the Department. I address these initiatives and the actions we are taking to respond to them in more detail in my written statement.

I would like to take this opportunity to highlight some of the steps we have taken and some of the immediate plans we are implementing to make these initiatives a permanent part of the security in the Department of Energy.

We have begun to review our design basis threat. A multi-discipline team has been formed and our Office of Intelligence has also already completed and delivered to that team a recent intelligence data that will assist them in ensuring that the DBT reflects current intelligence community understandings of the terrorist threat. By August 6th, the team will be prepared to present recommendations to the Secretary regarding any need changes to the DBT or to its implementing guidance.

Our cyber security teams and our systems, like everyone's, are under constant attack from the Internet. We are committed to finding and correcting our vulnerabilities to such attacks before anyone else can discover them. Under the Secretary's Red Teaming and Cyber Security Initiative, we are aggressively attacking our own systems and reporting the results to responsible managers. Under this initiative, our Cyber Security Oversight Office has already completed a Red Teaming assessment of one major site, and has already begun an assessment of another. These efforts will assist us in understanding exactly how attractive a target we represent, how we might be attacked in the future, and let us make any adjustments necessary to continue effective cyber operations in spite of these ongoing attacks.

We are very focused on consolidation of special nuclear material. If we can achieve a significant level of consolidation, we can be more efficient in both operations and security. A few months ago the Department formed a Consolidation of Materials Task Force to identify opportunities to relocate and consolidate special nuclear materials. They have already compiled and consolidated a list of excess material, a difficult and necessary step toward a comprehensive consolidation plan. In August, they will issue a report identifying short-term, which is 1 year, and long-term, beyond 1 year, options for consolidation and relocation. We are making progress in this area, but the balancing of programmatic cost and risk against security-related cost and risk is especially difficult. While everyone wants to see this effort finalized and implemented, we must allow adequate time to prepare a comprehensive plan that is prudent and affordable.

The Department has been concerned for some time that our Federal and contractor security experts were approaching retirement more quickly than new personnel could be recruited and trained. NNSA commissioned a group called the Chiles Commission, to recommend solutions within the NNSA Federal work force. That March report has identified a number of actions to address these issues with the NNSA Federal work force. The Secretary has directed that recommendations be considered for implementation among the remainder of the Federal security work force and applied as appropriate to contractor security workers as well. In support of this effort, our National Training Center, in Albuquerque, has been tasked to identify course and curriculum development actions that could provide better professional training for security specialists and managers. Their proposal is due on June 30th of this year.

I believe that the Department has not been as effective as it needs to be in deploying security technology to increase the effectiveness and efficiency of our protection efforts. This is not to say that we have not fielded some very useful technologies in the past. We have made innovative use of robot safes for S&M protection, special designed security doors, infrared devices, pressure sensitive intrusion sensors, and many more. Today we are working on activated denial system using non-legal levels of microwave energy that would make it impossible for adversaries to remain in the area, providing a great assistance to our implementing a denial strategy.

We are developing acoustic detective systems to improve our ability to inspect vehicles and large containers, and we are working with DOD to utilize some of their technology to produce beyond-the-fence early warning sensors that will scan areas beyond our perimeters to provide early warning of an attack. We are also investing in remotely controlled weapons that can be positioned in critical areas and operated by personnel located in hardened shelters where they are less susceptible to adversary fire. We continue to work on improved chemical agent countermeasures such as chemical agent detectors, chemically hardened patrol vehicles, and chemically hardened protective force ready rooms.

Since I last appeared before you, our Independent Oversight Office has completed three special reviews covering protective force management and capabilities, security lock and key programs, and security incident reporting programs. While these reviews began some time ago, they will influence many of the actions taken to address the Secretary's initiatives, particularly increasing training and standards for the Department's protective forces to an elite force and the increased use of keyless security entry systems and other technologies.

The Department is committed to real progress in every area of this security program. And, Congressman Watson, we are being more innovative and we are thinking out of the box now. But words and commitments are easy. Action is what counts. Today I have briefly described not only our plans and commitments, but also real actions taken and real progress made. I am confident that these, although significant, are just the beginning. Secretary Abraham

has provided us with a vision for the future and expects us to make that vision a reality.

With me today, who I had stand up at the swearing in, I have the Director of Security, Marshall Combs; I have the Director of Oversight, Mike Kilpatrick; I have the Office Director that was responsible originally for helping put the design basis threat together, who also co-chaired the special annex team, Larry Wilcher; and also Senior Physical Scientist Advisor, Dick Donovan.

Thank you.

[The prepared statement of Mr. Podonsky follows:]

STATEMENT OF

GLENN S. PODONSKY

DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSURANCE

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

JUNE 22, 2004

Statement of Glenn S. Podonsky
Director, Office of Security and Safety 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 22, 2004

Introductory Remarks

Mr. Chairman and honorable members of the subcommittee, I want to thank you for again inviting me to testify regarding safeguards and security programs in the Department of Energy. In previous testimony before this subcommittee on April 27th of this year, we presented detailed information regarding our process for developing and implementing the Department's Design Basis Threat; responded to the specific issues raised by the General Accounting Office in its draft report: *Nuclear Security: DOE Needs To Resolve Significant Issues Before It Fully Meets the New Design Basis Threat*; and described the role of my office, the Office of Security and Safety Performance Assurance, in the implementation of the Design Basis Threat and in other key efforts to improve security performance in the Department.

The information presented at the April 27th hearing remains valid, and therefore we offer no substantial amendments to that information today. However, significant activity having potentially far-reaching effects on the Department's protection programs has occurred in the two months that have elapsed since that previous testimony. Specifically, on May 7th Secretary Abraham delivered a major speech outlining his vision for the future of the Department's protection programs, and at the same time he announced a number of initiatives aimed at

implementing that vision. The Secretary's newly announced security initiatives will impact most major elements of our protection programs both in the Department at large and in the National Nuclear Security Administration, and it is those initiatives that we would like to address today.

The Secretary's Security Initiatives

Since assuming responsibility for the Department's management over three years ago, our senior managers have demonstrated a keen interest and close involvement in DOE's protection programs – and have not been shy about promoting actions to strengthen the programs and eliminate program weaknesses. Their personal interest and involvement has resulted in a number of actions that addressed a number of security concerns facing the Department. Understandably, senior management interest and involvement in security matters became even more focused after the terrorist attacks of 9/11. Since then, our understanding of the natures of the various threats we face has evolved, our protection program requirements have been adjusted to deal with the increased threats, we have changed some of our organizational relationships to improve security-related communication and cooperation between Headquarters and field elements, and our sites have taken the initiative to implement many local security measures to counter the increased threat. Our experiences in dealing with elevated threats and enhanced security postures since 9/11, and particularly our experiences with the immediate and long-term effects of manpower-intensive security enhancements, have led us to conclude that there are a number of additional steps we can and should take to increase the efficiency, effectiveness, and sustainability of our protection programs; hence, the Secretary's 14 new security initiatives. The complete set of new initiatives, as announced by Secretary Abraham, can be grouped into four broad program areas:

information security; new security technology solutions; consolidation of materials; and strengthening security human capital expertise. Together, they directly or indirectly impact every aspect of our protection programs.

Information Security

Much of what we do today is inextricably tied, in one way or another, to computers. A great deal of the information we possess, including classified information, is created on computers and/or stored on computer media. Most of our unclassified networks interface with the Internet. The fast pace of technological development of computer hardware and software seems to be equaled by the pace of development of methods to exploit that hardware and software for nefarious purposes. Cyber attacks, from large-scale information warfare campaigns to individual hacker vandalism, have become constant. The Department has been the target of cyber attacks in the past, and we will be targeted in the future. In fact, there is no doubt that many of our DOE computers and networks are under some level of cyber attack at this very moment. If we are to continue to operate effectively in the twenty-first century, we have to actively protect the confidentiality, integrity, and availability of all of the information on our automated systems, and we have to be able to do that even while we are under cyber attack. Consequently, we have to be on the cutting edge of cyber security. We need to employ tools, systems, procedures, and configurations that will provide the maximum degree of reliability and protection for our computer systems. Recognizing the urgency of this imperative and the potential consequences of falling behind in this area, the Secretary has resolved that even though the Department has made significant progress in cyber security programs in the past few years, we need to do more to

ensure that our protection systems keep abreast of emerging threats. Therefore, three of the new security initiatives focus on cyber security. These initiatives are specifically aimed at reducing the exposure of classified information stored on computer media; enhancing various individual aspects of our cyber security programs; and increasing the scope and volume of self-testing programs we use to identify (and eliminate) our own cyber vulnerabilities before an adversary does. While these initiatives include some longer-term developmental activities, many can be implemented in the near term, and some are already being implemented. The cumulative effects of these initiatives will significantly enhance our cyber protection abilities.

New Security Technology Solutions

In previous testimony before this subcommittee we stated that the DOE could and should make better use of security technologies to enhance our protection systems, and that evaluating new technologies and making them rapidly available to the field was one of my office's main focal areas. Properly applied, appropriate technologies can act as force multipliers to assist our protective forces by reducing the burden of routine activities, reducing the risk to them in case of an attack, and, through enhanced recognition combined with additional barrier delays, provide additional response time to meet and defeat an attack. Two of the Secretary's security initiatives are aimed specifically at enhancing our protection programs through increased use of technology.

One is directly responsive to several recent security incidents – specifically, replacing mechanical lock and key systems in security areas with modern, keyless entry control systems.

There have been relatively few actual incidents, but a recently concluded review by my Office of Independent Oversight and Performance Assurance clearly indicated the need for action to enhance the present level of control and accountability afforded keys and locks in the near term and the urgent need to move forward to implement the Secretary's initiative. Although simply replacing one type of lock with another may seem narrowly focused and easily achievable with current technology, this initiative is, in fact, a massive undertaking for an organization like DOE with the number of locks and keys currently in use at our security areas. The decision to move forward on this initiative represents a significant commitment on the part of the Secretary and the Department.

The other security technology initiative is a much broader and, in some ways, even more ambitious effort aimed at identifying, evaluating, or developing useful technologies and facilitating their timely implementation at appropriate DOE sites. We are particularly interested in evaluating and deploying emerging technologies that can help our protective forces better ascertain and thwart the ever-changing threats to our national security assets. We are examining emerging technologies being developed by the scientific community to determine if they have security utility, and if their benefits can be harnessed and applied within DOE. Examples of efforts currently underway include the development of an active denial system that will flood an area with microwave energy making it impossible for adversaries to carry out their objectives. Unlike a similar long range "battlefield" system being developed by the military, our effort focuses on a much shorter range version that can be deployed on the inside of facilities to provide a formidable barrier where special nuclear materials exist.

We are also investing in remotely controlled weapons that can be pre-positioned within secure areas, and activated by personnel located in hardened shelters where they are less susceptible to direct fire. One example of such a remotely controlled weapon is the TRAP system that we have identified for near-term deployment at several DOE sites. Test systems equipped with laser engagement systems have been tested in DOE facilities and have been found to be very effective. We have conducted a number of computer simulations of various deployment strategies for this system and these simulations have indicated that the TRAP system can be a substantial contributor. We are proceeding toward final deployment of this system as quickly as possible.

We are also investigating new sensor technologies to allow us to identify and engage adversaries farther from their target. We are investigating an acoustic device to assist us in conducting rapid, but thorough, searches of vehicles entering DOE sites. We are also working closely with the Department of Defense to bring some very promising beyond-the-fence early warning sensors into DOE. These sensors will help us scan areas outside of our perimeters to detect an attack long before the adversary can reach our most critical areas. The result will be an ability to identify and engage the adversary much earlier, giving us more time to bring the right weaponry and personnel to the fight.

In this area of technology application as well as in cyber security, we intend to stay on the cutting edge. The key to success in utilizing emerging security technologies to enhance DOE security, however, is not so much the availability of technology as our ability to identify appropriate technologies and field them in a timely manner. I am working with some of our most talented people to develop a better management model for identifying and fielding new

technologies than we have used in the past. If we are going to be successful in deploying technologies, we must be very innovative in our approach to this problem.

Consolidation of Materials

Special nuclear materials are among the most important national security assets entrusted to the Department's care. During the Cold War years, when we were engaged in building the nation's nuclear stockpile and in many other urgent national security-related activities, we needed and maintained large amounts of special nuclear materials at many sites throughout the complex. While we still need special nuclear materials at some sites to accomplish ongoing national security missions, both the amount of materials needed and the number of locations where they are needed have substantially decreased. Protecting these materials is among our most difficult security challenges, but we must protect these materials, since the consequences of their loss are unacceptable. We can greatly reduce the difficulty, risk, and costs associated with this mission by disposing of material we no longer need and consolidating the remainder in as few locations as operationally feasible. We have already made significant progress in consolidation efforts at sites that are being de-inventoried and decommissioned. However, much material that could be consolidated remains at sites where it is no longer needed for current or anticipated missions. This is largely because there is no place we have permission to send it or no authorized method of transporting it. We must resolve this issue. Additionally, we need to identify actual future needs for these materials, and identify what more we can do in the way of modifying or relocating operations to facilitate both mission requirements and further consolidation of materials. Since reduction/consolidation of special nuclear materials has perhaps the greatest

potential impact on our future protection requirements and programs, the Secretary has identified six separate initiatives related to this subject. These initiatives range in scope from developing plans for terminating a specific material-using reactor operation to determining the long-term needs and future configuration of the weapons complex. This group of initiatives goes directly to the heart of the challenges we face in our efforts to reduce and consolidate our special nuclear materials inventories and to protect these materials while in storage and in transit.

Strengthening Security Human Capital Expertise

Of all the components of our protection systems, the human component is the most critical, and the performance of our people will largely determine the success or failure of our protection efforts. Not to ignore the fact that virtually all of our Federal and contractor employees have security responsibilities, when we speak of security personnel in this context we refer to two groups of people: the people who design, implement, maintain, manage, and oversee the various elements of our protection programs; and the protective force personnel who are on the ground 24/7 guarding and defending our assets. The robustness and ultimate viability of our protection programs rests largely in the abilities and performance of these two groups of people. We have recognized the need to augment our current population of security specialists and to recruit and train the next generation of security specialists who will plan and manage our future protection systems. This need was reinforced by the recent findings and conclusions of a commission, headed by Admiral Henry Chiles, established by the NNSA Administrator to examine the security expertise issue within the NNSA. The Chiles Commission report clearly outlined a number of needs in this area, and recommended several actions to address these needs. The

Secretary has directed that these recommendations be extended, as appropriate, across the entire Department. Success in implementing this initiative will greatly strengthen the management and oversight of our safeguards and security programs.

Complex-wide, our protective forces have largely borne the brunt of our post-9/11 enhanced security efforts, many of which have been manpower intensive. The resulting overtime burden on protective force personnel has often been significant, and, to relieve that burden, training has often been reduced – sometimes to the minimum levels required to maintain essential minimum qualifications. We rely on our protective forces too much to allow this situation to continue. Although we have been successful in relieving this situation somewhat through additional hiring, expediting the security clearance process, employment of technology, and other efforts, we still see a need to strengthen and standardize protective force capabilities across the complex. Our Independent Oversight organization recently completed a comprehensive review of DOE protective forces that described current strengths and weaknesses exhibited by these forces. The review team found that line managers are supporting protective force tactical needs through efforts to procure enhanced weapons, ammunition, and equipment, and that performance during force-on-force performance tests indicated that our ability to protect special nuclear materials, always robust, continues to improve. However, there were also some systematic weaknesses identified that were fundamental in the formulation of the Secretary's announced vision of raising the training standards and performance standards of our protective forces to rival those of elite military forces.

While only three of the Secretary's initiatives deal with investing in safeguards and security human capital, I believe that the long term effects of our efforts here can rival the security impact of our technology-related initiatives. We don't have all the answers in this area yet, but we anticipate that the results of early actions on these initiatives will show us how to further strengthen the human components of our protection systems.

Implementing the Secretary's Security Initiatives

We understand that we will face some real challenges in managing and implementing these initiatives. They cover a broad range of activities, and they vary greatly as to the magnitude of effort each will require. For example, in anticipated level of effort they range from 90-day tasks to multi-year projects. However, we have already begun work on all of these security initiatives. The Secretary has formally tasked the appropriate organizations to plan for and begin implementation of the initiatives. The Department has developed Implementation Plans for each of the Secretary's fourteen security initiatives, which will be used to guide each activity through completion. But beyond plans, which are necessary prerequisites for these significant efforts, we have begun action on many of these initiatives. For example:

A review of our Design Basis Threat and associated threat assessments is already staffed and underway, and will be concluded by August 6th of this year. This is a multi-faceted review that focuses on five primary areas. First, the review is evaluating any changes in applicable intelligence information relating to adversary team sizes, compositions, and capabilities as well as any changes in radiological, chemical, and biological sabotage criteria that have occurred in

the past year since the publication of the DOE Design Basis Threat in May 2003. Second, the review is addressing recent concerns raised by Congress regarding protection strategies for special nuclear material that may be of improvised nuclear device concern in relation to the protection afforded other high-equity Departmental assets. Third, the team is examining whether GAO concerns regarding DBT implementation by FY2006 remain valid in light of recent budget request modifications. Fourth, the team is addressing any concerns with the 2003 DBT expressed by the field; and determining if any technical clarifications of the DBT or implementing guidance are necessary. Fifth, the team is examining the Department of Defense DBT and the associated implementation processes to ascertain if elements should and can be incorporated into the DOE DBT. The review team has completed the initial phase (identification and collection of relevant data) relating to each focus area. The DBT review team has entered the second phase (data analysis) of each focus area. By August 6th the review team will present recommendations to the Secretary, for his decision, regarding any needed changes to the Design Basis Threat or to its implementing guidance.

Our Independent Oversight organization is already taking action to increase the level of cyber security testing, including additional Red Team testing activities, enhanced classified system testing activities, and expanded and continuous scanning and penetration testing of unclassified networks. Our Office of Cyber Security and Special Reviews, utilizing its Cyber Security Testing Network facilities located in Germantown, Maryland and Columbus, Ohio, has begun enhanced red-team testing at DOE sites. Red team testing at one site has been completed and testing at another is well under way. We have also begun mapping DOE computers exposed to the Internet (mapping the DOE network perimeter), and demonstrating the capability to use

penetration testing tools and methodologies on classified networks. Additionally, we are benchmarking ourselves against the National Security Agency and will take advantage of some of that agency's training in approaches to exploitation of cyber system weaknesses.

The Department's "Consolidation of Nuclear Materials Task Force" has been formed and is at work pursuing its goals, which include: identifying opportunities for relocating/consolidating nuclear materials to reduce the number of potential targets; identifying legal, regulatory, and other issues that may impede relocation/consolidation of nuclear materials; identifying program efficiencies that can be achieved; and recommending short term (12 months) and long term (beyond 12 months) solutions to relocation/consolidation. The Task Force is due to issue its report with short term and long-term recommendations in August of this year. However, we are not waiting for the task force to complete its work and present its recommendations before we take action in cases where we have already identified material that we can or must relocate or consolidate. For example, the Secretary has already directed the removal of special nuclear material from TA-18 at Los Alamos National Laboratory; initial special nuclear material shipments are scheduled to begin in September.

NNSA has appointed an implementation team and commenced work to determine how best to implement the Chiles Commission's recommendations for improving our security human capital resources. In support of our human capital improvement initiative, our National Training Center has identified course and curriculum development actions that will be necessary to support additional professional training for security specialists and security managers. Some of these courses will be developed and available within six months.

While we need to be more aggressive in identifying and deploying current and emerging security technologies, the Department has already been active in this regard. The Department has fielded some countermeasures to possible adversary use of weapons of mass destruction, particularly to their use of chemical agents. We have fielded and will continue to field chemical agent protective personal protective equipment, around-the-clock chemical agent detectors, chemically hardened patrol vehicles, and chemically hardened protective force "ready rooms." We have already applied keyless access technologies at some of our most sensitive facilities and installation of such technologies is proceeding. The Department has already deployed diskless workstations in many of our classified networks where the capabilities of the currently available workstations are sufficient to perform necessary computational tasks.

This list of examples is not exhaustive, but it does serve to illustrate our commitment to security enhancements throughout what is already a very robust protection system.

Before I conclude my testimony, I would like to share an exciting development that we believe will significantly enhance our protective force performance testing and exercise programs. Our Office of Safeguards and Security Evaluations has, for over two decades, used force-on-force performance testing to evaluate protective force tactical capabilities and site protection strategies. Site protective forces have similar exercise programs, which they use for training purposes and to validate protection strategies and tactical plans. Recognizing the importance of an active tactical exercise program to the development and maintenance of protective force tactical

capabilities, subsequent to 9/11 the Secretary directed our sites to increase the frequency of their exercise programs.

Force-on-force exercises are very complex activities requiring substantial planning and resources. One aspect of the site protection program that we review very carefully during every safeguards and security inspection is the ability of the site to conduct an effective force-on-force performance-testing program. We have discovered that these exercise programs vary widely in quality throughout the complex. Some sites have not developed expertise, protocols, and databases adequate to support effective scenario development, exercise control, or evaluation. As a result, performance-testing programs at these sites are unable to properly evaluate their current forces or to support the evolution to an elite force.

We believe rigorous force-on-force performance testing against tough, skilled aggressor forces is one of the most important elements in measuring the effectiveness of our protective forces and in carrying us forward to an elite protective force. We are determined to do our part in advancing the Department's ability to conduct effective and informative force-on-force performance tests, as well as improving our ability to analyze the results of those tests. Therefore, we have decided to establish a Performance Test Center within the Office of Safeguards and Security Evaluations to facilitate our expansion of independent oversight performance testing activities and to establish standard protocols and databases that will be available to all sites for use in their internal exercise programs. This center will maintain standard protocols for all aspects of performance test planning, conduct, and safety for the entire DOE safeguards and security community. It will maintain databases and libraries necessary to support all aspects of

performance test planning, conduct, and control; scenario development; simulation; evaluation; and safety. For example, it will maintain databases on facility characterizations, ballistics effects, explosives effects, barrier delay times, chemical/biological effects, adversary capabilities, terrorist tactics and techniques, and simulation effects, to name a few. It will maintain safety tests and safety plans and protocols associated with appropriate weapons, ammunition, pyrotechnics, and equipment used in performance tests.

The center will work with the field and with our National Training Center to agree upon and formulate standardized versions of common activities, such as rules of engagement for exercise players, Controller rulings for various events, and minimum Controller training requirements. My staff is already working on the first initiatives that will be associated with the center, which include establishing common protocols for conducting rigorous performance tests across DOE and developing a database containing effects of explosives and other postulated adversary breaching techniques against common DOE defensive barriers. We are also laying the groundwork to provide input to the National Training Center curriculum on how to conduct force-on-force exercises and on how to role-play a determined adversary as realistically as possible. We expect to have some of the structural elements of the center, such as computer tactical scenario simulators, modeling software, and other basic analytical tools, in place by January 2005. This center will significantly streamline and enhance our own performance testing capabilities, and can provide similar benefits to sites that choose to draw on its resources for their internal exercise programs.

Concluding Remarks

In previous testimony before this committee, which dealt primarily with our revised Design Basis Threat, we expressed the belief that the Department's senior leadership was dedicated to improving our protection programs and was willing and determined to take the necessary steps to achieve that objective. Subsequent actions, including the Secretary's decision to implement fourteen far-ranging security initiatives and his direction to get to work quickly on all of them, have reinforced that belief. While at this point it is too early for these recent initiatives to have yet produced significant tangible results, the eventual fruits of these initiatives will be significant improvements in our protection programs.

We are confident that special nuclear materials and classified information are adequately protected throughout the complex. We also understand that portions of our protection programs need to be improved, and that the changing nature and capabilities of the threats we face may require further strengthening or realignment of protection program elements in the future. Implementation of the security initiatives we have discussed above will better enable us to respond to these needs. We of course have to follow through on these initiatives to ensure that they yield the expected concrete improvements in our protection programs. We believe that our line managers and staff are prepared to do so, and that the Department's senior managers will ensure that we do so.

Thank you. This concludes my prepared testimony.

Mr. TURNER. Thank you, Mr. Podonsky.

We will go through a 10-minute questioning period.

It strikes me, when you look at the title of this hearing, "Nuclear Security: Can DOE Meet Facility Security Requirements?", that we would not likely have a hearing that says DOE, too much security? So when we talk about the fact that at these particular facilities, that there is no margin for error, and that the support that you have for increased security is overwhelming, we want to make certain that if we are going to err, we err on the side of securing these facilities too much to meet whatever might face them. And no one is questioning DOE's commitment to this issue; it certainly is an issue of process and resources and decisionmaking.

Mr. Podonsky, I have a series of questions for you concerning this process of security-making decisions. You mentioned the design basis threat and the current review process that you are going through. Recognizing that the current design basis threat was written before you took over, the security policy functions, do you think the current design basis threat is robust enough?

Mr. PODONSKY. First, Congressman, thank you for asking me that question because, as you know, just 4 or 5 months ago, I was the director of Independent Oversight. I am on the record as criticizing the process of the Department's design basis threat. I am on the record as also criticizing the level of protection for INDs versus full-up weapons. Now that I am in charge of that policy organization, I would also tell you that we welcome the Secretary's initiative to have us take another look at the design basis threat; that was very necessary. In fact, I would tell you my policy organization, when it submitted its recommended design basis threat to the Secretary, Secretary Abraham himself raised the level up a couple of notches in terms of the numbers, without getting into specifics.

So I think it comes at a time that there needs to be an edited process, not a long bureaucratic one, but in today's threat that is looming on all of us every day, our families, our loved ones, our coworkers, it is vitally important that we get to what is the right level of protection that we need. And so the short answer would have been yes, I think it needed to be more robust. The longer answer is the Secretary recognizes that, and that is why he is having us take another look at this. And it is not just to review it and it is not a bureaucratic sense; we have an interagency group that is looking at other agencies. We have the intelligence briefings again, as recently as last Friday. So this is very active, it is not just standing there waiting for the next shoe to drop.

Mr. TURNER. I would like to also ask your thoughts, then, about the issues that we are hearing about the strain on the security forces, overtime, issues of training, equipment. Obviously we are hearing the long work hours that affect effectiveness. Could you speak to that?

Mr. PODONSKY. This concerns us as well, and a big part of this is part of the clearance process, getting the right security force on board, the numbers. But, Congressman, what we really think, it means that we need to have increased training; we have to have more technology applied. And let me just talk about technology. If we had more technology applied today—and there is technology on the shelf. This is not stop and study it, these technologies are

there—we can apply technologies, both developed for DOD as well as technologies developed in DOE, and help become force multipliers. For example, if you indulge me, I would like to give you an example. If we have a security member that is in a hardened position, that member, according to military doctrine, would be able to fight off a higher number, say seven or eight, attackers. If they are not in a hardened position, it becomes a shootout. And we think applying technology, increased weaponry will help reduce the strain on the existing force, because right now we are going forward with my army is bigger than yours. And SSA, our newly created office, what we want to impress upon the Department is not that my army is bigger than yours, my army is more technically qualified, competent with equipment, and trained properly, so we don't necessarily need the larger numbers of security forces, but a much more modern security force, an elite force, as the Secretary referred to in his May 7th announcements.

Mr. TURNER. Now getting to my favorite pet issue of the coordination between DOE and DOD. I appreciate your comments about additional technology equipment barriers that are being provided to the security forces. We frequently, in this discussion, hear the issue of gates, guns, and guards, and what would be the adequate sufficient number; and then the issue arises, as you have been discussing, of what technology would be appropriate to both make them more effective, safer, and lower the overall burden.

And recognizing that the security forces that are there are highly trained and are doing an excellent job at what they have been asked to do, it does strike me, whenever we look at this or whenever we have toured one of the facilities or discussed one of these facilities, that there does appear to be a limit as to what these security forces would be permitted to have with respect to equipment and technology, and that there is equipment and technology that would be available to DOD that would not be available to these security forces. Could you comment on that?

Mr. PODONSKY. One of the initiatives that we are moving out post-haste on is on the technology. There was an initiative that the Secretary called the Blue Sky technology project that Ambassador Brooks and I are teaming up on. Where we are moving out specifically is that my Security Office that Mr. Combs is director of has for many years utilized the laboratories for development of technologies. We are moving out to develop a, I don't want to call it a center of excellence, the Department uses that term too frequently and oftentimes is not a center of excellence at all, but we are moving out to develop a program where we put this technology, deploy it at sites right now. We are looking at technology being deployed at Pantex and at Y–12 as we speak. Technology has to be in the field to help the security forces today; not tomorrow, today. And we have the technology and we are applying that.

And I keep on coming back to the training as well. The training in the department for the security forces, as well as the white collar security professional, has been abysmal for the last 15 years. There hasn't been enough focus on that. Now, you may ask, well, why would we wait to train? Well, we have to train the security forces and the security managers to do their jobs, what they get paid to do, but we need to raise the bar in their training, we need

to combine that with the technology so that would help improve immensely those security forces, it will improve the overtime issues. It is all linked together. God forbid we call it a strategic plan.

Mr. TURNER. Mr. Podonsky, I appreciate your comments in answering my question concerning training and technology, and I know we don't want to go into, in this type of forum, a great deal of detail, but at the same time I remain concerned about the coordination between DOE and DOD, and the aspect of my question that you did not respond to is the issue of equipment. There is equipment that is not available to the security forces that is available through DOD. Isn't that correct?

Mr. PODONSKY. I believe there is some to that, yes.

Mr. TURNER. And that is where my concern comes, because I do believe that in this process of the design base threat, that there are bureaucratic walls where people do not allow themselves to pursue options because they would exceed the authority of the security forces that are there or the issues would be outside of the control purview of DOD. And I would just encourage you in that process not to look at those walls as impediments, but as opportunities.

Mr. PODONSKY. Congressman, if I might comment. You are correct, there needs to be better coordination between all the executive branch agencies in this regard, and both the legislative arm of Government as well as the executive branch is going to have to hold me back from kicking down those walls, because we don't believe in my SSA office that we have any time given to us. There is no error of margin allowable, and we have to move out. And I give credit to the Secretary. I have served seven secretaries, and this secretary has been very aggressive in security matters, and none like I have ever seen before. I am not a political, I am a career person, and I fervently believe that with the attention of this committee and a few other committees, as well as the attention of this Secretary, we will be able to break those barriers down, and not just through talk, we are going to do it through action, and we have already begun.

Mr. TURNER. Thank you.

Ms. Watson.

Ms. WATSON. As you address these various areas of concern, how are you going to affirm the effectiveness? Do we have to wait for an attack? Will you simulate various threats and attacks? How are we going to know if these new methods are going to be effective?

Mr. PODONSKY. Congresswoman Watson, currently we have an Office of Independent Oversight, and the operative word is independent; it does not have any financial connections to the other parts of the Department. Yes, it does report to the Secretary through my office, and that is an office that I ran for 20 years. And we have written about the performance of the Department on every subject, environment, safety, health, safeguard security, cyber security, emergency management; and all of those reports are very pronounced in terms of the actions that the Department must take. We will continue in a very robust fashion to have that office test all the sites, Mr. Garman's sites and Ambassador Brooks' sites.

We do not pull our punches, and if you are exposed to any of our briefings or any of the results of those inspections, you will see that we are extremely critical where we need to be on the Department.

Oftentimes the Department corrects the problems, and then there are times that it does not correct the problems, and for the last at least 12 years I have been coming up to Capitol Hill, briefing the various subcommittees on the results of those inspections.

What we have just completed right now in post-September 11 is a nationwide review of all of the protective force, because we wanted to, as you said in our last hearing, think out of the box. What are these protective forces thinking? What is the morale? How are they dealing? How are they going to deal when real bullets fly, as opposed to just laser tag. And so we just finished that report; we are going through that now, and we are going to be sharing that with the 200 secretaries and the deputy secretary. And that, we also believe, will contribute to what I was just saying before with Congressman Turner, to the training as well as the technology, how do we make these security forces better to protect the resources that they have at their command.

Ms. WATSON. Certainly we have the oversight, but we don't always get all the information, and I have taken on the role in my district, since I represent the largest city in California, and California has a lot of strategic ports, to carry information back to the people that are going to be involved and they have a responsibility too should there be an attack or whatever, but I don't feel that we really have had an opportunity to provide that oversight.

So I would like to hear from you how would you place what you feel are the real problems that we need to go after here, at this level, in terms of the whole system, the whole threat? How would you rank the problems that we should address?

Mr. PODONSKY. Well, again, this is my personal and professional opinion.

Ms. WATSON. That is what I am asking for.

Mr. PODONSKY. OK. And I would just say that it is long overdue that both the executive branch and the legislative arm of Government work hand in glove to oversee the security of the United States. Now, we have done that through the creation of Homeland Security; we have done that through recognition that the intelligence community needs to work better together with the FBI, etc. And I am not qualified to talk about all those on a professional level other than my personal opinion. What I have seen is there is a human factor problem, and that is we in this country sometimes have a short memory, Congresswoman, about all that happened on September 11. Right after September 11, we were all very wrapped up on what we needed to do, and over time we tend to forget that it is someplace else. And what we see everyday in the news and what is happening in Afghanistan and Iraq is very real. We have a war going on, and in order to protect cities like yours that you represent, there needs to be a check and balance on what the local authorities are doing in concert with the Federal Government, and there needs to be more of a collegial working together to solving the problems.

I realize that doesn't give you any specificity, but it is a beginning. And right now I don't think that we have that same drive universally around the country to fight terrorism except when it is right in front of us right that moment, and we should be prepared now, which is why the oversight of DOE, and I again compliment

Secretary Abraham, he puts a lot of confidence in the oversight function and he puts a lot of confidence in the security operation that he has just now created, SSA, to make a difference and to move the ball forward in all these areas that are needed that we heard this morning from both GAO and from the executive director of POGO.

Ms. WATSON. Well, maybe, Mr. Chairman, this committee should ask for the Secretary to give us an update on priorities and if there is a line item for budget going to be required. I am very compelled about the lack of trained staff, for instance, and the cost of training and vetting those who have been identified. And, you know, these processes do take time. Do we have time to meet the need? And so maybe we better, Mr. Chairman, this is very good, but maybe we better know where we are in terms of addressing these critical points.

With that, thank you, Mr. Chairman.

Mr. SHAYS [presiding]. I thank the gentlelady very much and appreciate her important questions and her participation as well.

Mr. Podonsky, I would like you, and then I am going to ask the professional staff to make sure we ask some questions that we need to get on the record. How would you compare security at the weapons sites versus the non-weapons sites? What represents the bigger challenge for us?

Mr. PODONSKY. Mr. Chairman, to answer your question, I would need to say that both ESE and NNSA both have category I, category II special nuclear material. The difference lies in a very pronounced difference, and that is NNSA has full-up nuclear weapons; ESE does not. However, ESE does have other challenges, and that is the reduction and closure of some of their sites. So where do they spend the money? For example, would they spend money on infrastructure, for example, a perimeter intrusion detection system for a site that was closing? I would think not. But then they still need to protect the material that they have. So the challenge that both Ambassador Brooks and Acting Under Secretary Garman face are very similar in terms of providing the appropriate security for the types of sites that they have, but I would say there are a lot of similarities, even though their missions are vastly different.

Mr. SHAYS. Thank you.

At this time I will ask Mr. Chase, of our staff, to ask some questions.

Mr. CHASE. Thank you, Mr. Chairman.

Secretary Garman, in your oral statement you said that it was your intention to monitor closely the implementation plans which are currently still under review. Understanding that, what challenges do you anticipate facing when you go about implementing these plans?

Mr. GARMAN. Of course, we will have the first of these implementation plans for the quarter ending June 30th, and they will be available prospectively. The problems that we are going to face is, of course, that in some areas vulnerability assessments at some sites have not yet been completed. Those sites would in fact include Argonne East and Brookhaven National Lab.

We are in a new situation where I don't believe we will ever reach what I would call security nirvana, where we can sit back,

relax, and say we have arrived. We are always going to be testing the system. We are always going to be trying to find where there are new threats, new vulnerabilities that we can uncover, and this is going to be a long and ongoing process.

The difficulty we have with ESE sites is that, in fact, a fundamental difference with the NNSA sites that have ongoing responsibilities for stockpile stewardship, many of our sites are trying to work themselves out of business. We are trying to consolidate the material, move it off the site, prepare the site for long-term legacy; and, as pointed out, you have to make a choice: do I want to spend $10,000 per linear foot for an intrusion protection system or do I want to quickly consolidate those materials or down-blend them, eliminating the threat altogether? That is where we are going to have the tussles, and that is where we need to be engaged.

The conflicts that I foresee between Mr. Podonsky's office and some of our online managers will be on this question of, and it has been stated here elegantly several times, how much security is enough, particularly if you are talking about a site that you are trying to close down more quickly. And if the perception is that you are taking financial resources to provide security that could at the same time be used to expedite or accelerate the cleanup of the site, therein we will have a conflict, and we are just going to have to work through those conflicts.

We have been able to do a good deal of special nuclear material consolidation at Mound, Rocky Flats, West Valley, Savannah River, but we obviously have a lot more to do.

So I would say that is the fundamental conflict I think we will see.

Mr. CHASE. As you know, the target date for implementation of the 2003 DBT is fiscal year 2006. GAO has indicated, I have heard this from folks at DOE, that fiscal year 2006 is probably not reasonable. Do you have any thoughts on that? When do you really think we are going to fully implement these plans?

Mr. GARMAN. We will know more as I see and review the implementation plans, but the Secretary and the Deputy Secretary have made it very clear to me that they believe fiscal year 2006 is what we need to be aiming for. That is certainly the requirement that I am going to place on the line managers reporting to me. As we review the quarterly assessments and understand where we are against those goals, we will have a better sense going forward. Obviously, there are some factors that I am concerned with outside our control. For example, will we receive in a timely way resources we ask for in the fiscal year 2006 budget, or will that be subject to continuing appropriations under what I think will be lower fiscal year 2005 levels? That is unknowable at this point, and it certainly is an element outside of my control or our control, but those are things that could have a bearing on our ability to meet that goal.

Also, Mr. Podonsky and his folks and others, from our Inspector General, are testing us, and we welcome this, trying to uncover new vulnerabilities that will teach us something we just don't know today, and that could have an impact. But right now I am not ready, or willing, to let our line managers off the hook for meeting the Secretary's guidance to meet these goals at the end of fiscal year 2006.

Mr. SHAYS. Mr. Podonsky, I realize that you gave an answer, and I am not quite sure I really could tell you what you told me, so I want to come back. Which site, the nuclear or the non-nuclear, present the greatest threat, and why?

Mr. PODONSKY. I understand the confusion in my answer, because I was answering my question, not yours. I would say that ESE has a tremendous challenge because of the areas that Mr. Garman just mentioned in terms of closure and the like, as well as NNSA has challenges for their sites. So I don't think, Congressman, that I could give you Garman's group or Brooks' group as being the greater challenge from our perspective. My oversight group has found an equal number of problems at both sets of sites. And having said that, we do feel that both organizations are attempting at various levels to fix those problems. There is a long way to go, I would say, at both organizations, both ESE as well as NNSA.

Mr. SHAYS. What is your biggest nightmare when you think about either these weapons or non-weapons sites?

Mr. PODONSKY. My biggest concern would be, from all the years of inspection, would be the weapons sites, with a footnote. We do have concerns on what a terrorist may or may not do with the materials that are within the borders of Mr. Garman's sites.

Mr. SHAYS. Do you have strong feelings in the work that you do about the need to close down some sites?

Mr. PODONSKY. Yes, sir, I do. I think that the Department could in fact take a serious look, and I know it is doing that in some sectors, of whether or not the footprint of the Department needs to be the size that it is now. So the consolidation of material is the first piece where we are identifying nuclear materials as excess that should be gotten rid of, and the consolidation of material that can be done on individual sites, and then perhaps the next step really should be whether we do need all the sites that are in the current DOE, that would be both NNSA and ESE.

Mr. SHAYS. Well, the fact is you know we don't need those sites.

Mr. PODONSKY. In my opinion we don't.

Mr. SHAYS. Right. But you have been around for how many years?

Mr. PODONSKY. Twenty years in August.

Mr. SHAYS. And your job is to anticipate what terrorists might do and have the antidote to it, correct?

Mr. PODONSKY. My job? Yes, sir.

Mr. SHAYS. And so one of the factors in doing that is consolidating the footprint of a particular site, getting rid of some of the obstructions, which may mean a reduction in people in some instances, but in the other instances it would actually be the elimination of some sites, correct?

Mr. PODONSKY. That is correct.

Mr. SHAYS. Is it fair to say that by having too many sites—I am not going to ask you specifically which ones you would say were too many, but by having too many sites, that it makes us more vulnerable?

Mr. PODONSKY. We clearly increase our vulnerabilities by having more targets out there.

Mr. SHAYS. And is it also true that if you were to reduce the number of sites, that you could be more focused on the ones that were left?

Mr. PODONSKY. I think common sense would lead you to that conclusion.

Mr. SHAYS. Common sense would, and that is why I am almost reluctant to ask it, because it is so obvious. But it is a fair statement to say that we are not yet spending all the resources we need to protect the sites that we have to the level that you believe we should protect them, correct?

Mr. PODONSKY. We are not there yet.

Mr. SHAYS. So if we had less sites, ultimately there would be a short-run increase in expenditures in some cases because we would have to consolidate, maybe build a little differently in other sites, tear down, so there would be some cost, but in the long run, if we consolidate, it would promise significant savings plus added security. Is that a statement you could agree with?

Mr. PODONSKY. From my perception, yes. But I must qualify one piece. I am not intimately familiar with all the programmatic aspects of the missions that are at all these sites, so that would also have to be part of the consolidation consideration.

Mr. SHAYS. Mr. Garman.

Mr. GARMAN. I just wanted to seek a point of clarification. Is the chairman talking about DOE sites generically or sites with nuclear material? Because therein lies the difference. Consolidation is part and parcel of what the ESE strategy is for dealing with this problem: consolidate the nuclear material at a smaller number of sites. That doesn't necessarily mean we want to eliminate certain sites. We have some sites, such as the National Renewal Energy Laboratory, that doesn't house nuclear material of any consequence, and I certainly wouldn't want them to be alarmed that we were talking about a site consolidation or elimination.

Mr. SHAYS. I think that is a fair point to make. I think in terms of base closings, we have 19 National Guard units that do artillery that we have testimony that they are just not needed, and yet we have overworked men and women in Iraq because of the skills they possess which are needed in Iraq. And I then think if someone told me that I had to have five offices in my district instead of the two I have, I could do that, but I would have to hire half as many people with twice as many sites.

And so what I want to do is bring to the level of dialog ultimately—we won't do it at this hearing—and that is when it is irresponsible for us to have so many sites both in our defense and so many sites in terms of our energy needs and what you, Mr. Garman, are responsible, and in terms of Mr. Podonsky, that these sites make us more vulnerable if they are not well protected. And having seen a few of them, I have seen old buildings that need to be torn down that don't have any use, I have seen the encroachment of the general public to these sites, and I was thinking, you know, the President doesn't have a lot of time to think about these things, so he is really trusting other people to do it for him. And then I realize there are political repercussions, but, you know, national security may dictate that we have people who are fairly outspoken, who say, you know, we need to do this.

Is there anything, Mr. Garman, that you would like to put on the record that we didn't put on the record?

Mr. GARMAN. Only the notion, and I certainly agree with this notion of consolidating materials. And we are going to need the help of Congress to do that. And also to dispose of materials. Plutonium disposition is a chronic problem in the Department, and it is something that we have been working on for a long time, and we will be working on it for a long time; down-blending highly enriched uranium. Consolidating materials, obviously, at a smaller number of sites means bringing materials such as highly enriched uranium and plutonium into sites and adding to the burden that those sites carry, which has political implications; it is why States and sites often fight us when we try to do consolidation efforts, because they say don't bring any more plutonium to our site. And so we will need the help of Congress to do this.

Mr. SHAYS. Well, you do need the help of Congress to do it, but we need to make sure that the folks that work in the bureaucracy, and I don't mean that in a bad way, but that work in our Government are telling us what we need to do. And I have been in public life now 30 years, and I am well aware of if you don't force the question, you give us the capability to deny knowledge, and then we are not held accountable. And so it just strikes me that we just need to make sure we have as honest a dialog as we can have. Put the burden on us, then the burden is on us.

Any other comment you want to make, Mr. Garman?

Mr. GARMAN. No, sir, other than to again express our thanks. You make us sharper by doing this, and we need this.

Mr. SHAYS. Well, thank you. Thank you.

Mr. Podonsky, any comment?

Mr. PODONSKY. Yes, sir. I appreciate that opportunity. I would just like to make a comment about the Secretary's initiatives. We have heard in testimony today that a lot of these initiatives, my terms, are retreads of the past, and some of that may be true; some of these initiatives maybe have been underway in different points. But again I want to emphasize never before have I seen at this agency such enthusiasm and focus to improve security as those 14 initiatives that the Secretary put forward. So I want to make sure that is clearly noted by the committee, that this is not just a retread, it is about action, and it is not about the department of plans anymore, it is a department of action.

Thank you, Mr. Chairman.

Mr. SHAYS. Thank you. I would like to ask you a question.

I do want to make sure that the Secretary's May 7th initiatives don't go unnoticed, and I would like to have a little dialog about it. One, it is, I think, a very positive step, and we appreciate it. How are we going to track the security initiatives? How will we go about doing that?

Mr. PODONSKY. We have set up a number of project teams that are looking at the milestones in the project plans for each one of these initiatives, and each one of these initiatives are supposed to be reported monthly to the Deputy Secretary in terms of the progress, and the Deputy Secretary has committed to get those briefings on a monthly basis. So this is going to be done by the existing corps of Federal employees, and it is a cross-representation

of both Mr. Garman's organization, Under Secretary Brooks, as well as my own.

Mr. SHAYS. Tell me, how did SSA get involved in the development of these initiatives?

Mr. PODONSKY. Quite a few months ago, Under Secretary Brooks and myself were asked, before Mr. Garman was put into the acting position, if we could come up with some out-of-the-box thinking of some initiatives to improve safeguard and security throughout the complex, and between our two organizations we gave the Secretary a menu of areas to look at, and the Secretary personally selected those 14 that he came up with, and we all supported those as real and something that was doable.

Mr. SHAYS. Was there anything left out that you wish had been included?

Mr. PODONSKY. No, sir. In fact, there was only one thing that I wish I didn't include.

Mr. SHAYS. OK, what was that?

Mr. PODONSKY. That was the Federalization of the guard force, because that has brought on more questions than I envisioned.

Mr. SHAYS. Mr. Garman, how are the security initiatives affecting ESE sites?

Mr. GARMAN. We are a full partner in the implementation of these. Tasking memorandum have been developed and sent out. Working groups are developing programs of action and milestones. Cyber security testing is underway, including at our sites. As Mr. Podonsky said, there are monthly reports tracking progress that are shared with me. ESE is actually leading one of the working groups involved in the consolidation of materials. And the Deputy and Administrator Brooks and I meet on a weekly basis, actually twice weekly, to go over some of these and other items that we have in common.

Mr. CHASE. Very quickly, Mr. Podonsky, in your written testimony, you made reference to the Chiles Commission report which was commissioned by Ambassador Brooks as it relates to the human capital expertise issue. Is there anything in that commission report that could be applied to ESE?

Mr. PODONSKY. Absolutely. Admiral Chiles' commission talks about the security training and qualifications of both the Federal staff as well as the protective force, and the findings in that report, while originally focused on NNSA, clearly Mr. Garman and his staff will be able to glean some golden nuggets out of that, as we in SSA are also taking out and taking very seriously, as I talked about in my testimony, in terms of the National Training Center in Albuquerque, so that we can raise the bar and the availability of training across the board for both uniform services as well as for the white collar security professionals.

Mr. SHAYS. Is there anything else either gentleman would like to put on the record?

Mr. GARMAN. Thank you, there is one item, and I will have to review the transcript to be sure of this, but at one point during the prior testimony I thought I heard the GAO witness, Ms. Nazzaro, suggest that there were ESE sites that were not subject to the DBT, or something along those lines. And I may have misheard it,

but I think what she was referring to was the DBT annex related to IND. I will review the transcript and try to be——

Mr. SHAYS. Well, why don't we just have someone just real quickly put that on the record. Do you want to just step up?

Mr. GARMAN. The only clarification I want to make is that all ESE sites are subject to DBT.

Mr. SHAYS. OK, and that is fine. And we all concur with that.

Mr. GARMAN. OK. Thank you.

Mr. SHAYS. Anything, Mr. Podonsky?

Mr. PODONSKY. No, sir.

Mr. SHAYS. And I would just put on the record thank you for waiting to take the second panel and just note for the record that the first panel has listened to your statements, so I appreciate that as well, so it works both ways.

And I thank both of you, and at this time this hearing is adjourned.

[Whereupon, at 11:25, the subcommittee was adjourned, to reconvene at the call of the Chair.]

○