DOE/ESE SECURITY: HOW READY IS THE PROTECTIVE FORCE

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JULY 26, 2005

Serial No. 109–104

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

25–259 PDF WASHINGTON : 2006

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*

CHRISTOPHER SHAYS, Connecticut
DAN BURTON, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
GIL GUTKNECHT, Minnesota
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
CANDICE S. MILLER, Michigan
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
GINNY BROWN-WAITE, Florida
JON C. PORTER, Nevada
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
CHARLES W. DENT, Pennsylvania
VIRGINIA FOXX, North Carolina

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
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
BRIAN HIGGINS, New York
ELEANOR HOLMES NORTON, District of Columbia

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*

KENNY MARCHANT, Texas
DAN BURTON, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEVEN C. LATOURETTE, Ohio
TODD RUSSELL PLATTS, Pennsylvania
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
JON C. PORTER, Nevada
CHARLES W. DENT, Pennsylvania

DENNIS J. KUCINICH, Ohio
TOM LANTOS, California
BERNARD SANDERS, Vermont
CAROLYN B. MALONEY, New York
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. DUTCH RUPPERSBERGER, Maryland
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York

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 July 26, 2005	1
Statement of:	
Aloise, Gene, Director, Natural Resources and Environment, Government Accountability Office, accompanied by James Noel, Assistant Director of Natural Resources and Environment, and Jonathan M. Gill, Senior Analyst, Natural Resources and Environment; Gregory H. Friedman, Inspector General, Department of Energy; Glenn S. Podonsky, Director, Office of Security and Safety Performance Assurance, Department of Energy; Dr. Lawrence Brede, Wackenhut, DOE Operations; Dr. Glenn Adler, Security Policy, Service Employees International Union; and Robert Walsh, Security Manager, Office of Energy, Science and Environment, Department of Energy	7
Adler, Dr. Glenn	73
Aloise, Gene	7
Brede, Dr. Lawrence	62
Friedman, Gregory H.	27
Podonsky, Glenn S.	40
Walsh, Robert	86
Letters, statements, etc., submitted for the record by:	
Adler, Dr. Glenn, Security Policy, Service Employees International Union, prepared statement of	76
Aloise, Gene, Director, Natural Resources and Environment, Government Accountability Office, prepared statement of	10
Brede, Dr. Lawrence, Wackenhut, DOE Operations, prepared statement of	64
Friedman, Gregory H., Inspector General, Department of Energy, prepared statement of	29
Grassley, Hon. Charles E., a Senator in Congress from the State of Iowa, prepared statement of	5
Podonsky, Glenn S., Director, Office of Security and Safety Performance Assurance, Department of Energy	43
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of	3
Walsh, Robert, Security Manager, Office of Energy, Science and Environment, Department of Energy:	
Followup question and response	110
Prepared statement of	89

DOE/ESE SECURITY: HOW READY IS THE PROTECTIVE FORCE

TUESDAY, JULY 26, 2005

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 10:05 a.m., in room 2154, Rayburn House Office Building, Hon. Michael Turner (chairman of the subcommittee) presiding.

Present: Turner, Shays, Burton, Marchant, Dent, Maloney, Kucinich, and Ruppersberger.

Staff present: Laurence Halloren, staff director and counsel; J. Vincent Chase, chief investigator; Robert Briggs, clerk; Sam Raymond and Eric Vaughn, interns; Andrew Su, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. TURNER. The hearing of the National Security, Emerging Threats, and International Relations hearing entitled, "DOE/ESE Security: How Ready is the Protective Force?," is called to order.

This hearing continues the subcommittee's examination of security programs at Department of Energy nuclear sites. Previous testimony described substantial institutional, technical and fiscal challenges confronting efforts to develop and implement a strengthened post-September 11th security standard called the design basis threat [DBT].

Today we focus on the substance and pace of DBT implementation at five sites outside the active weapons complex managed by the Department's Office of Energy, Science and Environment. Without question, ESE research labs and decommissioned sites are attractive targets for terrorists determined to turn our technology against us and willing to die while doing so.

The materials at these facilities pose a threat and can be used either as part of a weapon or a health threat directly. As DOE succeeds in hardening weapons production facilities and labs, ESE sites form the next tier of soft targets for nuclear terrorists following the path of least resistance.

But as we have heard before, ESE facilities housing substantial quantities of nuclear materials face unique problems implementing and sustaining enhanced security programs. The already vexing measure of how much security is enough against an uncertain threat becomes only more difficult when evaluating the costs and benefits of capital improvements and protective force enhance-

ments at decommissioned facilities DOE hopes to close sooner rather than later.

At the request of our chairman, Christopher Shays, the Government Accountability Office assessed the current readiness of protective forces at ESE sites and the steps still needed to defend those facilities against the larger, more capable attackers postulated in the DBT. Their findings, released today, point to a generally proficient guard staff prepared to meet existing standards. But the way forward to meet the higher DBT threat level is far less clear.

Efforts to deploy an elite protective force, utilize new security technologies and effectively manage ESE security initiatives require coordination and resource commitments that GAO is not sure will materialize. Plans to blend down and consolidate nuclear materials appear stymied by bureaucratic stovepipes and uncertain cost projections. Even under the best assumptions, security enhancements demanded by the 2004 DBT will not be completed before 2008, if then. The new security imperative demands implementation of a denial strategy to thwart access to nuclear materials, not just contain or catch intruders.

But in many ways, ESE seems stuck in denial about organizational and fiscal demands of a DBT-compliant strategy. Tactical training on assault scenarios lack vigor or realism. Communications equipment may be unreliable. Exceptions to training and equipment standards create inconsistencies and gaps in ESE safeguard systems. A diffused ESE security management structure frustrates efforts to implement and coordinate DOE-wide security policy securities.

Almost 4 years later, the undeniable realities of the post-September 11th world are not yet fully reflected in ESE security policies or practices. Our witnesses this morning will describe plans to implement the more stringent DBT and the steps needed to sustain those efforts against an undeniable dynamic threat. We appreciate their contribution to our ongoing oversight of DOE nuclear security, and we look forward to their testimony.

Gentlemen, as you are aware, it is the policy of this subcommittee to swear in our witnesses. If you would please stand and raise your right hands for the oath.

[Witnesses sworn.]

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

And I will acknowledge that Mr. Ruppersberger was in attendance at the commencement of this hearing. And I ask unanimous consent that all members of the subcommittee be permitted to place any 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, it is so ordered.

I ask further unanimous consent to place a statement from Senator Grassley, a co-requester on the GAO study to be discussed today, in the hearing record. Without objection, it is so ordered.

[The prepared statements of Hon. Christopher Shays and Hon. Charles E. Grassley follow:]

TOM DAVIS, VIRGINIA,
CHAIRMAN

CHRISTOPHER SHAYS, CONNECTICUT
DAN BURTON, INDIANA
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
GIL GUTKNECHT, MINNESOTA
E. SOUDER, INDIANA
V.C. LATOURETTE, OHIO
RUSSELL PLATTS, PENNSYLVANIA
S CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
CANDICE MILLER, MICHIGAN
MICHAEL R. TURNER, OHIO
DARRELL ISSA, CALIFORNIA
VIRGINIA BROWN-WAITE, FLORIDA
JON C. PORTER, NEVADA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
CHARLES W. DENT, PENNSYLVANIA
VIRGINIA FOXX, NORTH CAROLINA

ONE HUNDRED NINTH 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

http://reform.house.gov

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
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
BRIAN HIGGINS, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA

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
July 26, 2005

This hearing continues the Subcommittee's examination of security programs at Department of Energy (DOE) nuclear sites. Previous testimony described substantial institutional, technical and fiscal challenges confronting efforts to develop and implement a strengthened, post-9/11 security standard called the "Design Basis Threat" (or "DBT").

Today we focus on the substance and pace of DBT implementation at five sites, outside the active weapons complex, managed by the Department's Office of Energy, Science and Environment (ESE). Without question, ESE research labs and decommissioned sites are attractive targets for terrorists determined to turn our technology against us, and willing to die while doing so. The highly enriched uranium and plutonium held at these locations could be used as the core of an improvised nuclear device or dispersed as a radiological weapon. As DOE succeeds in hardening weapons production facilities and labs, ESE sites form the next tier of soft targets for nuclear terrorists following the path of least resistance.

But, as we've heard before, ESE facilities housing substantial quantities of nuclear materials face unique problems implementing and sustaining enhanced security programs. The already vexing measure of "How much security is enough against an uncertain threat?" becomes only more difficult when evaluating the costs and benefits of capital improvements and protective force enhancements at decommissioned facilities DOE hopes to close sooner than later.

At our request, the Government Accountability Office (GAO) assessed the current readiness of protective forces at ESE sites and the steps still needed to defend those facilities against the larger, more capable terrorist cells postulated in the DBT. Their findings, released today, point to a generally proficient guard staff prepared to meet existing standards.

But the way forward to meet the higher DBT threat level is far less clear. Efforts to deploy an elite protective force, utilize new security technologies and effectively manage ESE security initiatives require coordination and resource commitments that GAO is not sure will materialize. Plans to down-blend and consolidate nuclear materials appear stymied by bureaucratic stovepipes and uncertain cost projections. Even under the best assumptions, security enhancements demanded by the 2004 DBT will not be completed before 2008, if then.

The new security imperative demands implementation of a "denial strategy" to thwart access to nuclear materials, not just contain or catch intruders. But in many ways, ESE seems stuck in denial about the organizational and fiscal demands of a DBT-compliant strategy. Tactical training on assault scenarios lacks rigor and realism. Communications equipment may be unreliable. Exceptions to training and equipment standards create inconsistencies and gaps in ESE safeguard systems. A diffuse ESE security management structure frustrates efforts to implement and coordinate DOE-wide security policies.

Almost four years later, the undeniable realities of the post-9/11 world are not yet fully reflected in ESE security policies or practices. Our witnesses this morning will describe plans to implement the more stringent DBT and the steps needed to sustain those efforts against an undeniable, dynamic threat. We appreciate their contribution to our ongoing oversight of DOE nuclear security and we look forward to their testimony.

Statement by Senator Chuck Grassley of Iowa

Before the House Government Reform Subcommittee on National Security, July 26, 2005

I want to thank Chairman Shays for his leadership on oversight and his continued interest and commitment to such an essential part of what we do here in Congress. Today's hearing will shine the spotlight on an issue Chairman Shays and I raised over two years ago –the security of our nation's nuclear labs. Congressman Shays has been conducting oversight on these issues since October 2001. We teamed up in May 2003 to get answers to the many questions that are addressed in the report that is the focus of today's hearing.

On June 24, 2003, I testified before this very committee over my concerns that our nation's nuclear labs might be in harm's way. These labs are critical research and development facilities for weapons design, weapons grade nuclear material and other highly classified programs. In a world where terrorists, criminals and spies often find their way to our doorstep, we cannot afford to allow these nuclear labs to become vulnerable.

At the request of Congressman Shays and myself, the U.S. Government Accountability Office (GAO) has conducted an extensive study of the security at some of these facilities. The Design Basis Threat (DBT) is a classified document that identifies the potential size and capabilities of adversary forces. These guidelines are then used to determine to what extent the protective forces are meeting existing Department of Energy requirements. The DOE has made a decision not to require full compliance with the Design Basis Threat until October 2008. This allows time for each of the facilities to make the needed changes in their protective forces in order to meet that threat.

The GAO points out in their study that to successfully defend against a larger terrorist threat, the Department of Energy needs to take "several prompt and coordinated actions." Their study revealed that 85 out of 105 protective force officers interviewed feel that their current training is not adequate to prepare them for the standards set by the 2008 DBT. The DOE has responded by proposing the development of an elite force, similar to our military's Special Forces. I believe that the Department of Energy should take the appropriate steps necessary to ensure that the protective forces get the training and equipment they need to do their job successfully.

The GAO also revealed that the DOE is currently in the process of reviewing new technology that could be used to defend and counter potential attacks on those facilities. These labs produce some of the world's most advanced technology, yet many of the protective force officers interviewed admit having unreliable and outdated communications systems. In addition to that, many of the protective forces lack modern-day equipment, such as the latest body armor and chemical protective gear.

Another issue addressed by the GAO is the "down-blending" or consolidation of nuclear material between and among the various Energy, Science and Environment (ESE) sites.

The idea that we could move nuclear material from a less secure facility to a more secure facility appears to be promising. I would welcome additional facts and figures concerning the feasibility of such a plan.

Finally, the study indicated that the headquarters of the ESE may not be organized properly to handle security issues. Apparently, there was no "centralized security organization" within the Office of the Under Secretary of Energy, Science and Environment until June 2005, at which time the Acting ESE Security Director, David Garmen, was confirmed and later sworn in as the Under Secretary of ESE. I am optimistic that we now have a permanent position that will oversee these critical issues. The clock is ticking, and there is an urgent need to have a person in place who will evaluate the recommendations of the GAO and make the right decisions.

Mr. Chairman, I think you will agree with me when I say there is no time to waste. The cost of failure is too high. The problems identified over the last two years are not beyond repair. But all needed repairs must be made promptly. I hope we are not sitting here in 2008 discussing why the DOE, ESE and NNSA cannot meet the updated Design Basis Threat.

Thank you for your patience and leadership, Mr. Chairman.

Mr. TURNER. Our witnesses today for this panel include Mr. Gene Aloise, Director, Natural Resources and Environment, Government Accountability Office, accompanied by Mr. James Noel, Assistant Director of Natural Resources and Environment; and Mr. Jonathan M. Gill, Senior Analyst, Natural Resources and Environment.

We also have Mr. Gregory H. Friedman, Inspector General, Department of Energy; Mr. Glenn S. Podonsky, Director, Office of Security and Safety Performance Assurance, Department of Energy; Dr. Lawrence Brede, Wackenhut, DOE Operations; Dr. Glenn Adler, security policy, Service Employees International Union [SEIU]; and Mr. Robert Walsh, Security Manager, Office of Energy, Science and Environment, Department of Energy.

And if I have mispronounced any of your names, please correct the record when you give your testimony.

We will begin our testimony with Mr. Aloise.

STATEMENTS OF GENE ALOISE, DIRECTOR, NATURAL RESOURCES AND ENVIRONMENT, GOVERNMENT ACCOUNTABILITY OFFICE, ACCOMPANIED BY JAMES NOEL, ASSISTANT DIRECTOR OF NATURAL RESOURCES AND ENVIRONMENT, AND JONATHAN M. GILL, SENIOR ANALYST, NATURAL RESOURCES AND ENVIRONMENT; GREGORY H. FRIEDMAN, INSPECTOR GENERAL, DEPARTMENT OF ENERGY; GLENN S. PODONSKY, DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSURANCE, DEPARTMENT OF ENERGY; DR. LAWRENCE BREDE, WACKENHUT, DOE OPERATIONS; DR. GLENN ADLER, SECURITY POLICY, SERVICE EMPLOYEES INTERNATIONAL UNION; AND ROBERT WALSH, SECURITY MANAGER, OFFICE OF ENERGY, SCIENCE AND ENVIRONMENT, DEPARTMENT OF ENERGY

STATEMENT OF GENE ALOISE

Mr. ALOISE. Mr. Chairman and members of the subcommittee, I am pleased to be here today to discuss our work on nuclear security at DOE's Energy, Science, and Environment sites. A terrorist attack on one of these sites, containing weapons-grade nuclear material could have devastating consequences for the site and nearby communities.

Mr. TURNER. Excuse me. These mics are relatively directional. Could you pull the mic forward? And if you would twist it just a bit so that it is pointed directly at you, that would help us.

Mr. ALOISE. These consequences could include theft of nuclear material, explosion of an improved nuclear device, and use of the material in a dirty bomb. To protect these sites, an effective security program is essential.

DOE's security program begins with a document known as the "design basis threat," which identifies the size and capabilities of potential adversaries. The 2004 design basis threat identified a much larger terrorist threat than before, and it could cost between about $400 million and $600 million to develop the force necessary to defeat this larger threat.

DOE is allowing its sites until October 2008 to fully meet the new design basis threat. My remarks, which are based on the re-

port we are issuing for the subcommittee today, will focus on whether ESE protective forces are meeting current readiness requirements and what actions are needed to defend against a larger October 2004 design basis threat.

Regarding readiness, we found that protective forces at the five ESE sites, with weapons-grade nuclear material, generally meet readiness requirements. Specifically, protective forces at the Savannah River site, Hanford site, Idaho, and Argonne West, and Oak Ridge National Lab generally comply with DOE standards for firearms proficiency, physical fitness and equipment, and had the required training programs and facilities.

However, we did find weaknesses that could impact the protective forces' ability to defend their sites. For example, most officers we spoke with were concerned about the quality and realism of their training. Further, because DOE neither sets standards for, nor tracks individual participation in force-on-force exercises, it was difficult to determine how many officers had this important training.

Another weakness identified by protective force officers at all five sites concerned problems with their radios. Some said that the radios could not be relied on in the event of a terrorist attack.

In addition, although most protective forces are required to have access to body armor, at one site we found that body armor had not been issued for most officers. Another site did not have its own special response team. In the event of an attack, one of the jobs of a special response team would be to recover stolen nuclear material.

In addition, the capability of some of the protective forces to fight during a chemical or biological attack varied. Specifically, two sites expected and provided equipment for most of their forces to fight in contaminated areas. Another site did not provide any equipment. Indeed, it expected its teams to evacuate the site with other workers. Yet another site expected its forces to fight in a chemically contaminated area, but did not provide protective gear.

Another weakness we observed was that only one of the five sites had armored vehicles. In contrast, all six NNSA sites with weapons-grade nuclear material have armored vehicles.

Now regarding actions needed to meet the 2004 design basis threat. In our view, DOE needs to develop and implement a comprehensive Department-wide plan which addresses, among other things, the transition to an elite fighting force, investments in emerging security technologies, and the consolidation of weapons-grade nuclear material. Further, DOE needs to establish a centralized security office within ESE to help meet the challenges of implementing the new design basis threat.

While I am pleased to note that DOE has accepted our report recommendations, DOE's response to our recommendation to develop a comprehensive plan to meet the new design basis threat does not go far enough. DOE has cited only individual efforts to address the new threat, and not the larger plan we are calling for. Without such a plan, DOE may not be successful in meeting the requirements of the 2004 design basis threat by October 2008.

Mr. Chairman, this concludes my remarks. I would be happy to respond to any questions you or members of the subcommittee may have.

[NOTE.—The July 2005 GAO report entitled, "Nuclear Security, DOE's Office of the Under Secretary for Energy, Science and Environment Needs to Take Prompt, Coordinated Action to Meet the New Design Basis Threat, GAO–05–611," may be found in subcommittee files.]

[The prepared statement of Mr. Aloise follows:]

United States Government Accountability Office

GAO

Testimony

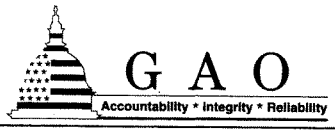
Before the Subcommittee on National Security, Emerging Threats and International Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, July 26, 2005

NUCLEAR SECURITY

Actions Needed by DOE to Improve Security of Weapons-Grade Nuclear Material at its Energy, Science and Environment Sites

Statement of Gene Aloise, Director
Natural Resources and Environment



GAO-05-934T

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-934T, a testimony before the Subcommittee on National Security, Emerging Threats and International Relations, Committee on Government Reform, House of Representatives

Why GAO Did This Study

A successful terrorist attack on a Department of Energy (DOE) site containing nuclear weapons material could have devastating effects for the site and nearby communities. DOE's Office of the Under Secretary for Energy, Science and Environment (ESE), which is responsible for DOE operations in areas such as energy research, manages five sites that contain weapons-grade nuclear material. A heavily armed security force equipped with such items as automatic weapons protects ESE sites. GAO was asked to examine (1) the extent to which ESE protective forces are meeting DOE's existing readiness requirements and (2) the actions DOE and ESE will need to take to successfully defend against the larger, revised terrorist threat identified in the October 2004 design basis threat (DBT) by DOE's implementation deadline of October 2008.

What GAO Recommends

To ensure that DOE and ESE protective forces can meet the terrorist threat contained in the 2004 DBT, GAO made five recommendations to the Secretary of Energy to, among other things, address weaknesses with protective officers' equipment and coordinate ESE efforts to address the 2004 DBT. DOE concurred with and accepted GAO's recommendations and provided an update on actions it anticipated taking to address GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-05-934T.

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

July 26, 2005

NUCLEAR SECURITY

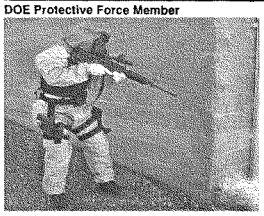
Actions Needed by DOE to Improve Security of Weapons-Grade Nuclear Material at its Energy, Science and Environment Sites

What GAO Found

Protective forces at the five ESE sites containing weapons-grade nuclear material generally meet existing key DOE readiness requirements. Specifically, GAO determined that ESE protective forces generally comply with DOE standards for firearms proficiency, physical fitness levels, and equipment standardization and that the five ESE sites had the required training programs, facilities, and equipment. However, GAO did find some weaknesses at ESE sites that could adversely affect the ability of protective forces to defend these sites. For example, despite the importance of training exercises in which protective forces undergo simulated attacks by a group of mock terrorists (force-on-force exercises), DOE neither sets standards for individual protective force officers to participate in these exercises, nor does it require sites to track individual participation. GAO also found that protective force officers at all five of the ESE sites reported problems with their radio communications systems. Specifically, according to 66 of the 105 protective force officers GAO interviewed, they did not always have dependable radio communications as required by the DOE Manual 473.2-2, *Protective Force Program Manual*. Security officials stated that related improvements were under way.

To successfully defend against the larger terrorist threat contained in the 2004 DBT by October 2008, DOE and ESE officials recognize that they will need to take several prompt and coordinated actions. These include transforming its current protective force into an elite, possibly federalized, force, developing and deploying new security technologies to reduce the risk to protective forces in case of an attack, consolidating and eliminating nuclear weapons material between and among ESE sites, and creating a sound ESE management structure that has sufficient authority to ensure coordination across all ESE offices that have weapons-grade nuclear material. However, because these initiatives, particularly an elite force, are in early stages of development and will require significant commitment of resources and coordination across DOE and ESE, their completion by the October 2008 DBT implementation deadline is uncertain.

DOE Protective Force Member



Source: DOE

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the work you requested on nuclear security at the Department of Energy's (DOE) Office of the Under Secretary for Energy, Science and Environment (ESE). My testimony is based on the report being released today, entitled *Nuclear Security: DOE's Office of the Under Secretary for Energy, Science and Environment Needs to Take Prompt, Coordinated Action to Meet the New Design Basis Threat* (GAO-05-611).

DOE has long recognized that a successful terrorist attack on a site containing the material used in nuclear weapons, such as plutonium or highly enriched uranium, could have devastating consequences for the site and its surrounding communities. The risks associated with these materials, which in specified forms and quantities are referred to as Category I special nuclear material, vary but include theft for use in an illegal nuclear weapon; the creation of improvised nuclear devices capable of producing a nuclear yield; and the creation of so-called "dirty bombs," in which conventional explosives are used to disperse radioactive material.

Because terrorist attacks could have such devastating consequences, an effective safeguards and security program is essential. For many years, a key component for DOE security programs has been the development of the design basis threat (DBT), a classified document that identifies the potential size and capabilities of adversary forces. In response to the September 11, 2001, terrorist attacks, DOE issued an updated DBT in May 2003 and gave its sites until October 2006 to comply with its requirements. In response to recommendations in our April 2004 report to this Subcommittee,[1] congressional criticism, and a new review of intelligence data, DOE issued a revised DBT in October 2004. The 2004 DBT identified a larger terrorist threat for DOE sites than the 2003 DBT. Consequently, DOE is not requiring full compliance with the 2004 DBT until October 2008 in order to allow its sites adequate time to implement measures to defeat this larger terrorist threat. By July 29, 2005, DOE sites will have to forward 2004 DBT implementation plans to the Deputy Secretary of Energy and, within 3 months, begin submitting quarterly DBT implementation reports. At the time of our review, cost estimates were still preliminary, but

[1]See GAO, *Nuclear Security: DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat*, GAO-04-623 (Washington, D.C.: Apr. 27, 2004).

security officials at ESE sites said that, collectively, they may require an additional $384 million-$584 million over the next several years in order for all ESE sites with Category I special nuclear material to meet the 2004 DBT.

The private contractors who operate DOE's facilities counter the terrorist threat contained in the DBT with a multifaceted protective system. While specific measures vary from site to site, a key universal component of DOE's protective system is a heavily armed protective force equipped with such items as automatic weapons, night vision equipment, body armor, and chemical protective gear.

On June 22, 2004, we testified before this Subcommittee, identifying several issues that could impede ESE's ability to fully meet the threat contained in the May 2003 DBT by DOE's October 2006 deadline.[2] Not the least of theses issues was the lack of a departmentwide, multiyear, fully resourced implementation plan for meeting DBT requirements; the plan would have to include important programmatic activities, such as the closure of facilities and the transportation of special nuclear material.

Subsequently, you asked us to examine ESE in more detail and to determine, for the five ESE sites with Category I special nuclear material, (1) the extent to which ESE protective forces are meeting DOE's existing readiness requirements and (2) what actions DOE and ESE will need to take to successfully defend against the larger, revised terrorist threat identified in the October 2004 DBT by DOE's implementation deadline of October 2008.

To determine the extent to which protective forces at ESE sites are meeting existing DOE readiness requirements, we reviewed pertinent literature about the factors that affect the readiness of forces, such as military forces, that are like those defending ESE sites. We conducted structured interviews with 105 randomly selected ESE protective force officers at the five ESE sites that contain Category I special nuclear material. While the responses from these interviews are not projectable to the entire universe of ESE protective force officers, we did speak to about 10 percent of the total protective forces at the five sites. We asked the

[2]See GAO, *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*, GAO-04-894T (Washington, D.C.: June 22, 2004).

officers questions designed to determine their readiness to defend the sites, including questions about their morale, training, and equipment. We also reviewed the training records of the 105 officers for selected firearms and physical fitness qualifications to determine if these officers complied with existing DOE requirements and regulations. Finally, we reviewed the equipment used by ESE protective forces to determine if it met current DOE requirements.

To determine what actions DOE and ESE will need to take to successfully defend against the new threat identified in the October 2004 DBT by DOE's implementation deadline of October 2008, we reviewed the October 2004 DBT and associated guidance documents. We discussed the October 2004 DBT with officials in DOE's Office of Security and Safety Performance Assurance and with officials in ESE's Offices of Environmental Management; Nuclear Energy, Science and Technology; and Science, which oversee the five ESE sites that contain Category I special nuclear material. Finally, where available, we reviewed documents prepared by ESE officials on how they plan to comply with the October 2004 DBT. We performed our work between March 2004 and July 2005 in accordance with generally accepted government auditing standards.

In summary, we found the following:

- Protective forces at the five ESE sites containing Category I special nuclear material generally meet existing DOE readiness requirements. However, we did find some weaknesses at ESE sites that could adversely affect the ability of ESE protective forces to defend their sites. With respect to current readiness, 102 of the 105 officers we interviewed stated that they believed that they and their fellow officers understood what was expected of them if the site were attacked by a terrorist group. Moreover, 65 of the 105 officers rated themselves as highly ready to defend their site while 20 officers rated themselves as somewhat or moderately ready. Supporting their views, we found that the five ESE sites we visited had the required training programs, facilities, and equipment, and that the 105 protective force members whose records we reviewed generally complied with existing DOE standards for firearms proficiency, physical fitness levels, and equipment standardization. However, we did find some weaknesses at ESE sites that could adversely affect the ability of protective forces to defend these sites. For example, despite the importance of training exercises in which protective forces undergo simulated attacks by a group of mock terrorists (force-on-force exercises), DOE neither sets standards for individual protective force officers to participate in these exercises, nor requires sites to track individual

participation. While 84 of the 105 protective force officers we interviewed stated they had participated in a force-on-force exercise, only 46 of the 84 protective force officers believed that the force-on-force exercises they had participated in were either realistic or somewhat realistic. We also found that protective force officers at all five of the ESE sites reported problems with their radio communications systems. Specifically, according to 66 of the 105 protective force officers we interviewed, they did not always have dependable radio communications, as required by DOE Manual 473.2-2, *Protective Force Program Manual*. Site security officials stated that improvements were underway and would be completed this year.

- To successfully defend against the larger terrorist threat contained in the 2004 DBT by October 2008, DOE and ESE officials recognize that they will need to take several prompt and coordinated actions. These include transforming its current protective force into an "elite force"—modeled on U.S. Special Forces, developing and deploying new security technologies to reduce the risk to protective forces in case of an attack, consolidating and eliminating nuclear weapons material between and among sites, and creating a sound ESE management structure that has sufficient authority to ensure coordination across all ESE offices that have Category I special nuclear material. However, these initiatives, particularly an elite force, are in the early stages of development and will require a significant commitment of resources and coordination across DOE and ESE. Consequently, their completion by the 2008 October DBT implementation deadline is uncertain.

In our report to you we made five recommendations to the Secretary of Energy to track and increase protective force officers' participation in force-on-force training exercises, correct weaknesses with protective force officers' equipment, coordinate implementation of DOE's various efforts designed to meet the 2004 DBT through the development of a departmentwide, multiyear implementation plan, and create a more effective ESE security organization.

DOE concurred with our report, accepted our recommendations and provided an update on actions it anticipated taking to address our recommendations. While we believe that most of DOE's anticipated actions will be responsive to our recommendations, we are concerned about DOE's response to our recommendation that it develop a departmentwide, multiyear implementation plan for meeting the 2004 DBT requirements. Specifically, in responding to this recommendation, DOE cited only individual efforts to address the development of an elite force, the deployment of enhanced security technologies, and the consolidation

of special nuclear material, not the development of a departmentwide, multiyear implementation plan. While each of these efforts is important, we continue to believe that DOE cannot be successful in meeting the requirements of the 2004 DBT by its deadline of October 2008 without an integrated effort that is built around a comprehensive plan.

Background

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

- the Savannah River Site near Aiken, South Carolina, and the Hanford Site in Richland, Washington, which are managed by the Office of Environmental Management;
- the Idaho National Engineering and Environmental Laboratory and the Argonne National Laboratory-West, which are located in Idaho Falls, Idaho, and are managed by the Office of Nuclear Energy, Science and Technology[3]; and
- the Oak Ridge National Laboratory in Oak Ridge, Tennessee, which is managed by the Office of Science.

Contractors operate each site for ESE. DOE has requested over $300 million in fiscal year 2006 for security at these five sites.

Within DOE's Office of Security and Safety Performance Assurance, DOE's Office of Security develops and promulgates orders and policies to guide the department's safeguards and security programs. DOE's overall security policy is contained in DOE Order 470.1, *Safeguards and Security Program*, which was originally approved in 1995. The key component of DOE's approach to security is the DBT, a classified document that identifies the characteristics of the potential threats to DOE assets. A classified companion document, the *Adversary Capabilities List*, provides additional information on terrorist capabilities and equipment. The DBT traditionally has been based on a classified, multiagency intelligence community assessment of potential terrorist threats, known as the *Postulated Threat*. The threat from terrorist groups is generally the most demanding threat contained in the DBT.

[3]The two Idaho sites were consolidated as a single site, now known as the Idaho National Laboratory, in February 2005.

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 the following:

- a variety of integrated alarms and sensors capable of detecting intruders;
- physical barriers, such as fences and antivehicle obstacles;
- numerous access control points, such as turnstiles, badge readers, vehicle inspection stations, radiation detectors, and metal detectors;
- operational security procedures, such as a "two person" rule that prevents only one person from having access to special nuclear material; and
- hardened facilities and vaults.

Each site also has a heavily armed protective force that is often equipped with such items as automatic weapons, night vision equipment, body armor, and chemical protective gear. These protective forces are comprised of Security Police Officers who are classified into three groups: Security Police Officer-I, Security Police Officer-II, and Security Police Officer-III. Security Police Officer-Is are only assigned to fixed, armed posts. Generally, very few of these officers are used at ESE sites because of the limited roles they can fill. Security Police Officer-IIs generally are assigned to posts such as access control booths, or to foot or vehicle patrols. Finally, Security Police Officer-IIIs are responsible for operations such as hostage rescue and the recapture and recovery of special nuclear material. According to federal regulations, Security Police Officer-IIIs have more demanding physical fitness and training standards than Security Police Officer-Is or Security Police Officer-IIs. The ESE sites we visited employ about 1,000 Security Police Officer-IIs and Security Police Officer-IIIs. ESE protective forces work for private contractors and are unionized.

Protective force duties and requirements, such as physical fitness standards, are explained in detail in DOE Manual 473.2-2, *Protective Force Program Manual*, as well as in DOE regulations (10 C.F.R. pt. 1046, *Physical Protection of Security Interests*). DOE issued the current *Protective Force Program Manual* in June 2000. Although protective forces are expected to comply with the duties and requirements established in DOE policies, deviations from these policies are allowed as long as certain approval and notification criteria are met.

In addition to complying with these security requirements, DOE protective systems, including protective forces, also must meet performance standards. For example, DOE sites are required to demonstrate that their protective systems are capable of defending special nuclear material against terrorist forces identified in the DBT. The performance of protective systems 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 exercises, in which the site's protective forces undergo simulated attacks by a group of mock terrorists. In addition to their use in evaluating the effectiveness of physical protection strategies, DOE believes force-on-force exercises are the most realistic representation of adversary attacks that can be used to train protective forces.

Protective Forces at ESE Sites Generally Meet Established DOE Readiness Requirements, but Some Weaknesses in Protective Force Practices Exist

Protective forces at the five ESE sites containing Category I special nuclear material generally meet existing key DOE readiness requirements. Specifically, we determined that ESE protective forces generally comply with DOE standards for firearms proficiency, physical fitness levels, and equipment standardization and that the five ESE sites had the required training programs, facilities, and equipment. In addition, we found that the majority of the 105 protective force members we interviewed at ESE sites generally believe that they currently are ready to perform their mission of protecting the site's special nuclear material. However, we did find some weaknesses at ESE sites that could impair the ability of ESE protective forces to defend their sites.

Protective Force Officers Are Confident in Their Current Overall Readiness and Generally Meet the DOE Training and Equipment Requirements We Reviewed

A ready force should possess a sufficient number of experienced, trained, and properly equipped personnel. Through realistic and comprehensive training, these personnel are forged into a cohesive unit that can perform its tasks even under extreme conditions. DOE orders and federal regulations establish the framework for ensuring that DOE protective forces are ready to perform their mission. We found that ESE protective force officers generally believe that they are ready to perform their mission. Specifically, 102 of the 105 officers we interviewed stated that they believed that they, and their fellow officers, understood what was expected of them should the site be attacked by a terrorist group. Moreover, 65 of the 105 officers rated the readiness of their site's

protective force as high, while 20 officers rated their protective force as somewhat or moderately ready to defend the site. Only a minority of the officers (16 of 105) we interviewed rated the readiness of their force to defend their sites as low. In addition, the majority of officers we interviewed believed they and the protective force officers with whom they worked on a regular basis have formed a cohesive unit that would be able to perform their most essential mission—that of protecting special nuclear material. For example, of the 105 officers we interviewed, 84 officers responded that they had a high degree of confidence in their fellow officers in the event of a terrorist attack, and 88 reported that their fellow officers would be willing to risk their lives in defense of their site.

As called for in DOE's *Protective Force Program Manual*, readiness is achieved through appropriate training and equipment. Each of the five sites we visited had formally approved annual training plans. Each site generally had the training facilities, such as firearms ranges, classrooms, computer terminals, and exercise equipment, which enabled them to meet their current DOE and federal training requirements. Furthermore, each site maintained computerized databases for tracking individual protective force officers' compliance with training requirements. To determine if these programs and facilities were being used to implement the DOE requirements and federal regulations, we focused on three key areas—firearms proficiency, physical fitness, and protective force officer equipment.

- *Firearms Proficiency.* DOE's *Protective Force Program Manual* states that protective force officers must demonstrate their proficiency with the weapons that are assigned to them every 6 months. According to the training records of the 105 protective force officers we interviewed, 79 had met this proficiency requirement with their primary weapon, the M-4 or M-16 semiautomatic rifle. Of the 26 officers who had not met this requirement within the 6 month time frame, 11 officers were all located at one site and 8 of these 11 officers did not meet the requirement until 2 to 5 months after the required time. According to an official at this site, seven of the eight officers could not complete the requirement in a timely fashion because the site's firing range was closed for the investigation of an accidental weapon discharge that had resulted in an injury to a protective force officer. We determined that 2 of the 26 officers did not complete the requirement for medical reasons. We were not given reasons why the remaining officers did not meet the requirement.

- *Physical Fitness.* Under DOE regulations,[4] DOE's contractors' protective force personnel who are authorized to carry firearms must meet a minimum standard for physical fitness every 12 months. There are two standards for such personnel—Offensive Combative and Defensive Combative. All Security Police Officer-IIIs, which include DOE special response team members, must meet the Offensive Combative standard, which requires a 1-mile run in no more than 8 minutes 30 seconds and a 40-yard prone-to-running dash in no more than 8 seconds. All other protective officers authorized to carry firearms must meet the Defensive Combative standard, which requires a one-half mile run in no more than 4 minutes 40 seconds and a 40-yard prone-to-running dash in no more than 8.5 seconds. According to the training records of the 105 protective force officers we reviewed, 103 of the 105 protective force officers had met the standard required by federal regulation for their position. Two officers who did not meet the requirement were on medical restriction. The records for another officer showed him as having met the requirement, but additional records provided by the site showed the officer had completed the run in a time that exceeded the standard. Site officials could not provide an explanation for this discrepancy.

- *Protective Officer Equipment.* DOE's *Protective Force Program Manual* sets a number of requirements for protective force equipment. For example, all Security Police Officers are required to carry a minimum set of equipment, including a portable radio, a handgun, and an intermediate force weapon such as a baton. In addition, a mask to protect against a chemical attack must be carried or available to them. All Security Police Officer-IIs and Security Police Officer-IIIs must also have access to personal protective body armor. In addition, firearms must be kept serviceable at all times and must be inspected by a DOE-certified armorer at least twice a year to ensure serviceability. Issued firearms must be inventoried at the beginning of each shift, an inventory of all firearms in storage must be conducted weekly, and a complete inventory of all firearms must be conducted on a monthly basis. Finally, DOE protective forces equipment must be tailored to counter adversaries identified in the DBT. To this end, sites employ a variety of equipment, including automatic weapons, night vision equipment, and body armor. In most cases, each site's protective forces carried or had access to the required minimum standard duty equipment. Most sites demonstrated that they had access to certified armorers, and each site maintained the required firearms maintenance, inspection, and inventory records, often kept in a detailed

[4] 10 C.F.R. pt. 1046, subpt. B, app. A.

computerized database. The appropriate policies and procedures were also in place for the inventory of firearms. In addition, some sites have substantially increased their protective forces weaponry since September 11, 2001, or have plans to further enhance these capabilities to meet the 2004 DBT.

Some Weaknesses in ESE Site Protective Force Practices Exist

While protective forces at ESE sites are generally meeting current DOE requirements, we identified some weaknesses in ESE protective force practices that could adversely affect the current readiness of ESE protective forces to defend their sites. These include protective force officers' lack of participation in realistic force-on-force exercises; the frequency and quality of training opportunities; the lack of dependable communications systems; insufficient protective gear, including protective body armor and chemical protective gear; and the lack of armored vehicles.

- *Performance Testing and Training.* According to DOE's *Protective Force Program Manual*, performance tests are used to evaluate and verify the effectiveness of protective force programs and to provide needed training. A force-on-force exercise is one type of performance test during which the protective force engages in a simulated battle against a mock adversary force, employing the weapons, equipment, and methodologies postulated in the DBT. DOE believes that force-on-force exercises are a valuable training tool for protective force officers. Consequently, DOE policy requires that force-on-force exercises be held at least once a year at sites that possess Category I quantities of special nuclear material or Category II quantities that can be rolled up to Category I quantities. However, DOE neither sets standards for individual protective force officers' participation in these exercises, nor requires sites to track individual participation. While 84 of the 105 protective force officers we interviewed stated they had participated in a force-on-force exercise, only 46 of the 84 protective force officers believed that the force-on-force exercises they had participated in were either realistic or somewhat realistic. Additionally, protective force officers often told us that they did not have frequent and realistic tactical training. In this regard, 33 of the 84 protective force officers reported that safety considerations interfered with the realism of the force-on-force exercises, with some protective force officers stating that they were limited in the tactics they could employ. For example, some protective force officers stated that they were not allowed to run up stairwells, climb fences, or exceed the speed limit in patrol vehicles. Contractors' protective force managers agreed that safety requirements limited the kind of realistic force-on-force training that are needed to ensure effective protective force performance.

- *Communications Equipment.* According to DOE's *Protective Force Program Manual*, the radios protective force officers use must be capable of two-way communications, provide intelligible voice communications, and be readily available in sufficient numbers to equip protective force personnel. In addition, a sufficient number of batteries must be available and maintained in a charged condition. Protective force officers at all five of the sites we visited reported problems with their radio communications systems. Specifically, 66 of the 105 protective force officers reported that they did not always have dependable radio communications, with 23 officers identifying sporadic battery life, and 29 officers reporting poor reception at some locations on site as the two most significant problems. In addition, some of the protective force officers believed that radio communications were not sufficient to support their operations and could not be relied on if a terrorist attack occurred. Site security officials at two sites acknowledged that efforts were under way to improve radio communications equipment. In addition, security officials said other forms of communications, such as telephones, cellular telephones, and pagers, were provided for protective forces to ensure that they could communicate effectively.

- *Protective Body Armor.* DOE's *Protective Force Program Manual* requires that Security Police Officer-IIs and -IIIs wear body armor or that body armor be stationed in a way that allows them to quickly put it on to respond to an attack without negatively impacting response times. At one site, we found that most Security Police Officer-IIs had not been issued protective body armor because the site had requested and received in July 2003 a waiver to deviate from the requirement to equip all Security Police Officer-IIs with body armor. The waiver was sought for a number of reasons, including the (1) increased potential for heat-related injuries while wearing body armor during warm weather, (2) increased equipment load that armor would place on protective force members, (3) costs of acquiring the necessary quantity of body armor and the subsequent replacement costs, and (4) associated risks of not providing all Security Police Officer-IIs with body armor could be mitigated by using cover provided at the site by natural and man-made barriers. According to a site security official, this waiver is currently being reviewed because of the increased threat contained in the 2004 DBT.

- *Special Response Team Capabilities.* Security Police Officers-IIIs serve on special response teams responsible for offensive operations, such as hostage rescue and the recapture and recovery of special nuclear material. Special response teams are often assigned unique equipment, including specially encrypted radios; body armor that provides increased levels of protection; special suits that enable officers to operate and fight in

chemically contaminated environments; special vehicles, including armored vehicles; submachine guns; light machine guns; grenade launchers; and precision rifles, such as Remington 700 rifles and Barrett .50 caliber rifles. These response teams are also issued breaching tools to allow them to reenter facilities to which terrorists may have gained access. Each site with Category I special nuclear material must have a special response team capability available on a continuous basis. However, one ESE site does not have this capability and, instead, relies on another organization, through a formal memorandum of understanding, to provide a special response team. This arrangement, however, has not been comprehensively performance-tested, as called for in the memorandum of understanding. Site officials state that they will soon conduct the first comprehensive performance test of this memorandum of understanding.

- *Chemical Protective Gear.* DOE's *Protective Force Program Manual* specifies that all Security Police Officer-IIs and -IIIs be provided, at a minimum, with protective masks that provide for nuclear, chemical, and biological protection. Other additional chemical protective gear and procedures are delegated to the sites. At the four sites with special response teams, we found that the teams all had special suits that allowed them to operate and fight in environments that might be chemically contaminated. For Security Police Officers-IIs, chemical protective equipment and expectations for fighting in chemically contaminated environments varied. For example, two sites provided additional protective equipment for their Security Police Officer-IIs and expected them to fight in such environments. Another site did not provide additional equipment but expected its Security Police Officer-IIs to evacuate along with other site workers. Finally, the one site that did not have a special response team expected its Security Police Officer-IIs to fight in chemically contaminated environments. However, the site provided no additional protective gear for its officers other than standard-duty issue long-sleeved shirts and the required protective masks.

- *Protective Force Vehicles.* We found that ESE sites currently do not have the same level of vehicle protection as National Nuclear Security Administration (NNSA) sites that also have Category I special nuclear material. Specifically, while not a DOE requirement, all NNSA sites with Category I special nuclear material currently operate armored vehicles. However, only one of the five ESE sites with Category I special nuclear material operated armored vehicles at the time of our review. One other ESE site was planning to deploy armored vehicles.

DOE and ESE Officials Need to Take Several Prompt and Coordinated Actions to Address the New DBT Requirements by 2008

To successfully defend against the larger terrorist threat contained in the 2004 DBT by October 2008, DOE and ESE officials recognize that they need to take several actions. These include transforming its current protective force into an elite force, developing and deploying new security technologies, consolidating and eliminating special nuclear material, and making organizational improvements within ESE's security program. However, because these initiatives, particularly an elite force, are in early stages of development and will require a significant commitment of resources and coordination across DOE and ESE, their completion by the October 2008 DBT implementation deadline is uncertain. The status of these initiatives is as follows:

- *Elite Forces.* DOE officials believe that the way its sites, including those sites managed by ESE, currently train their contractor-operated protective forces will not be adequate to defeat the terrorist threat contained in the 2004 DBT. This view is shared by most protective force officers (74 out of 105) and their contractor protective force managers who report that they are not at all confident in their current ability to defeat the new threats contained in the 2004 DBT. In response, the department has proposed the development of an elite force that would be patterned after U. S. Special Forces and might eventually be converted from a contractor-operated force into a federal force. Nevertheless, despite broad support, DOE's proposal for an elite force remains largely in the conceptual phase. DOE has developed a preliminary draft implementation plan that lays out high-level milestones and key activities, but this plan has not been formally approved by the Office of Security and Safety Performance Assurance. The draft implementation plan recognizes that DOE will have to undertake and complete a number of complex tasks in order to develop the elite force envisioned. For example, DOE will have to revise its existing protective forces policies to incorporate, among other things, the increased training standards that are needed to create an elite force. Since this proposal is only in the conceptual phase, completing this effort by the October 2008 DBT implementation deadline is unlikely.

- *New Security Technologies.* DOE is seeking to improve the effectiveness and survivability of its protective forces by developing and deploying new security technologies. It believes technologies can reduce the risk to protective forces in case of an attack and can provide additional response time to meet and defeat an attack. Sixteen of the 105 protective force officers we interviewed generally supported this view and said they needed enhanced detection technologies that would allow them to detect adversaries at much greater ranges than is currently possible at most sites. However, a senior DOE official recently conceded that the department has not yet taken the formal steps necessary to coordinate investment in

emerging security technologies and that the role of technology in helping sites meet the new threats contained in the 2004 DBT by the department's deadline of October 2008 is uncertain.

- *Consolidation and Elimination of Materials.* ESE's current strategy to meet the October 2008 deadline relies heavily on consolidating and eliminating special nuclear material between and among ESE sites. For example, the Office of Nuclear Energy, Science and Technology plans to down-blend special nuclear material and extract medically useful isotopes at the Oak Ridge National Laboratory—an Office of Science site. This action would eliminate most of the security concerns surrounding the material. Neither program office, however, has been able to formally agree on its share of additional security costs, which have increased significantly because of the new DBT. In addition, neither ESE nor DOE has developed a comprehensive, departmentwide plan to achieve the needed cooperation and agreement among the sites and program offices to consolidate special nuclear material, as we recommended in our April 2004 report. In the absence of a comprehensive plan, completing most of these consolidation activities by the October 2008 DBT implementation deadline is unlikely.

- *Organizational Improvements.* The ESE headquarters security organization is not well suited to meeting the challenges associated with implementing the 2004 DBT. Specifically, there is no centralized security organization within the Office of the Under Secretary, ESE. The individual who serves as the Acting ESE Security Director has been detailed to the Office by DOE's Office of Security and Safety Performance Assurance and has no programmatic authority or staff. This lack of authority limits the Director's ability to facilitate ESE and DOE-wide cooperation on such issues as material down-blending at Oak Ridge National Laboratory and material consolidation at other ESE sites.

Mr. Chairman, this concludes my prepared statement. I 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 Gene Aloise at (202) 512-3841. James Noel, Jonathan Gill, Don Cowan, and Preston Heard made key contributions to this testimony.

GAO's Mission

The Government Accountability 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 GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

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. Government Accountability 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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Mr. TURNER. Thank you.
Mr. Friedman.

STATEMENT OF GREGORY H. FRIEDMAN

Mr. FRIEDMAN. Mr. Chairman and members of the subcommittee, I am pleased to be here, at your request, to testify on recent reviews conducted by the Office of Inspector General regarding security programs of the Department of Energy. This is the latest in a series of testimonies that we have provided to the Congress on this important subject. The issues addressed have included training, physical security, and performance testing. A number parallel those addressed in GAO's just issued report.

Between 2003 and 2005, we identified issues regarding protective force overtime and training. In one review, which included five Department sites, we found the Department faced significant increases in unscheduled protective force overtime. Further, we noted protective force morale and retention problems due to mandatory overtime and reduced training opportunities.

In a review with the Department's Oak Ridge Reservation, we found that contractor protective force personnel spent, on average, about 40 percent less time on combat readiness refresher training than that specified in the training plan approved by Federal site managers, and that the personnel worked in excess of the Department's optimum 60-hour per week threshold.

In a third review we found that 10 of the 12 sites made significant modifications to the Department's established protective force core curriculum. This raised questions about the effectiveness of the training received by the affected protective force personnel, as well as the validity of the core curriculum.

In June 2005, we examined physical security at two DOE facilities. In the first review we found that foreign construction workers using false identification documents gained access to the Oak Ridge Y–12 National Security Complex. During our field work, management issued a revised access policy. Nonetheless, we were concerned, and are concerned, that similar conditions may exist at other sensitive Department sites. Therefore, we recommended that management determine whether agency-wide actions are warranted.

The second review concerns security at the Strategy Petroleum Reserve. The Reserve, which the Department has designated as part of its critical infrastructure, contains about 695 million barrels of oil valued at about $36 billion. We concluded that physical security at the Reserve could be improved.

Specifically, we found that 87 percent of the non-protective force contractor employees of the Reserve, some with the ability to access sensitive areas unescorted, had never been processed for any level of security clearance. Therefore, in our judgment, the Reserve's level of protection against the "insider threat" may not be consistent with its critical infrastructure designation. We also found the Reserve's deadly force policy may also not be consistent with the Reserve's critical infrastructure designation; and, finally, we identified opportunities to make site protective force performance tests more realistic.

Protective force performance testing was also the subject of a January 2004 report, where we found that a performance test at Y–12 was compromised as a result of certain protective force personnel being allowed to view computer simulations of the test scenarios prior to the test, and there was an apparent pattern of actions by Oak Ridge Reservation security personnel going back to the mid-1980's that may have negatively affected the reliability of site performance tests.

In another 2004 report concerning Oak Ridge, we identified that the two local Department management offices, the Oak Ridge office and the Y–12 site office, were developing separate radio communications projects. The two projects as designed would have created gaps in radio coverage and would have prevented Y–12 protective forces from maintaining communications with the rest of the Oak Ridge Reservation and their own dispatcher.

These findings were similar to an earlier review at four other Department sites, in which we found that three of the four sites did not have direct radio communication with local law enforcement agencies. These agencies would have been called upon to assist in the pursuit of suspected felons or terrorists fleeing Department sites.

We also have a number of ongoing and planned security reviews relevant to the topics discussed during this hearing. This includes an intensive effort to review the Department's security program and its progress in meeting the threat posed in the revised design basis threat document.

The Department is working to address many security concerns and is doing so at a substantial cost. The Office of Inspector General will continue to examine the Department's security apparatus with the goal of providing recommendations to enhance efficiency and effectiveness.

Mr. Chairman and members of the subcommittee, this concludes my statement. I would be pleased to answer any questions.

[The prepared statement of Mr. Friedman follows:]

STATEMENT OF GREGORY H. FRIEDMAN
INSPECTOR GENERAL
U. S. DEPARTMENT OF ENERGY

BEFORE THE
U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY,
EMERGING THREATS, AND INTERNATIONAL RELATIONS

FOR RELEASE ON DELIVERY
Tuesday, July 26, 2005

Good morning Mr. Chairman and members of the Subcommittee. I am pleased to be here at your request to testify on the readiness of the Department of Energy's energy, science, and environment sites to successfully defend against the terrorist threat identified in the Department's October 2004 Design Basis Threat document.

Since 1997, the Office of Inspector General has reported security as one of the Department of Energy's most significant management challenges. This was based on the body of work that we have done in this area, the sensitivity of the Department's operations, and evolving threat assessments. Consequently, the Office of Inspector General devotes a significant portion of its resources to reviewing the effectiveness of security programs and operations at Department of Energy facilities. The result has been numerous findings and recommendations designed to enhance Department security.

I would like to highlight several recent Inspector General reports that address current security issues, including:

- protective force training and management,
- facility access controls,
- physical security,
- cyber security,
- protective force performance testing, and
- protective force communications.

A number of our issues parallel those addressed in the July 2005 draft Government Accountability Office report on protective forces at the Department's energy, science, and environment sites.

The Department's Basic Protective Force Training Program

The Department's contractors employed over 4,100 security officers responsible for protecting Department sites. Of this number, approximately 1,650 security officers served at energy, science, and environment sites.

The Department's policy is to train its security forces to deal with a broad range of threats and ensure interoperability across the complex. In March 2004, we completed a review to determine whether sites were meeting the requirements of the Department's standardized, basic protective force core training curriculum. In our report, "The Department's Basic Protective Force Training Program" (DOE/IG-0641), we noted that 10 of the 12 sites we reviewed had made significant modifications to the Department's established protective force core curriculum. Five of the 10 sites were energy, science, and environment facilities that store or had stored special nuclear material. Specifically:

- Each of the 10 sites eliminated or modified 2 or more blocks of instruction from the core curriculum;
- Seven sites reduced the intensity of hands-on training for skills that some security experts characterized as critical, such as handcuffing, hand-to-hand combat, and vehicle assaults; and

- None of the 10 sites included instruction in rappelling, which is a core curriculum course for special response team training.

We noted that some modifications occurred because site security managers questioned the applicability of certain courses or had related safety concerns. These modifications were not always detected or their impact on readiness assessed by the respective program offices or the Office of Security because the Department did not require sites to report changes made to the core training requirements.

The high number of modifications to the protective force core curriculum raised questions about the validity of the curriculum and may lead to an increase in the risk that the Department's protective forces will not be fully trained to carry out their security responsibilities.

Management concurred with our recommendations to review curriculum modifications and agreed to issue additional guidance defining when the Department should be notified about modifications.

Protective Force Training at the Department of Energy's Oak Ridge Reservation

In June 2005, we issued a report on "Protective Force Training at the Department of Energy's Oak Ridge Reservation" (DOE/IG-0694). We determined that contractor protective force personnel spent, on average, about 40 percent less time on combat

readiness refresher training than that specified in the training plan approved by Federal site managers. This included training in areas such as team tactical exercises, chemical and biological warfare, vehicle assault, handgun malfunctions, and the use of force.

We also found that protective force personnel worked in excess of 60 hours per week, despite a 60-hour maximum threshold for safe operations established in the Department's Protective Force Program Manual. In particular, protective force personnel at the Y-12 National Security Complex routinely worked in excess of 60 hours per week.

Management, in concurring with the report's findings and recommendations, stated that it intended to review the adequacy of protective force refresher training at Department sites, as well as the acceptability of deviations from the annual training plans for core protective force skills. Management also stated that the reduction of overtime continues to be a significant goal at Oak Ridge.

Management of the Department's Protective Forces

In June 2003, we raised training and overtime concerns in a report on the "Management of the Department's Protective Forces" (DOE/IG-0602). To the Department's credit, we found that in the post-September 11, 2001, period, improvements had been made in the management of its protective force program. However, we noted that the Department faced a number of challenges that could adversely affect the program. Specifically, we reviewed five sites, and we observed:

- Significant increases in unscheduled protective force overtime;
- Protective force morale and retention problems based on mandatory overtime and reduced training opportunities; and
- Long delays associated with granting clearances for newly employed protective force officers.

In the report, we recognized that the Department of Energy, like other Government agencies, faced security challenges relative to the unanticipated demand for additional security personnel immediately after September 11, 2001. We concluded, however, that in subsequent years, the Department had the opportunity to improve the operation of its protective force program by taking advantage of accelerated methods of processing security clearances for officers, incorporating specific performance metrics into protective force contracts, and developing an overall protective force contingency strategy.

In responding to the report, Department management stated that it had launched an initiative to enhance protective force management, including the use of expedited processing of security clearances for protective force personnel.

Security Access Controls at the Y-12 National Security Complex

In June 2005, we completed a review of an allegation that non-U.S. citizens were improperly allowed access to a leased facility at the Department's Y-12 National Security

Complex, which is an integral component of the Department's nuclear weapons program. In a report on "Security Access Controls at the Y-12 National Security Complex" (DOE/IG-0691), we found that foreign construction workers used false identification documents, which resulted in their gaining access to Y-12 facilities.

During our review, management at Y-12 issued a revised access policy. Nevertheless, we were concerned that similar findings may exist at other sensitive Department sites. Therefore, we recommended that management determine whether Department-wide actions were warranted. In response, management stated that future security inspections of Department facilities will include reviews of access control procedures.

Review of Security at the Strategic Petroleum Reserve

The Strategic Petroleum Reserve serves as the Nation's first line of defense against an interruption in petroleum supplies. The Reserve contains approximately 695 million barrels of oil valued at about $36 billion.

In our June 2005 report on "Review of Security at the Strategic Petroleum Reserve" (DOE/IG-0693), we concluded that additional measures could be implemented to improve physical security at Reserve sites. Management agreed with our findings and recommendations and agreed to implement corrective actions. Specifically, we found that:

- The level of protection against the "insider threat" at the sites may not be consistent with the designation of the Reserve as part of the Department's

critical infrastructure. Of the non-protective force contractor employees at the Reserve, 87 percent had never been processed for any level of security clearance. Some of these employees were allowed unescorted access to sensitive areas.

- Similarly, the Reserve's deadly force policy may not be consistent with the Reserve's critical infrastructure designation.
- Finally, opportunities existed to make protective force performance tests at the Reserve more realistic. Specifically, we found that the Reserve's security condition threat level is often elevated for certain tests, which provides for additional protective force personnel to defend the site during the tests.

This performance test finding was similar to the findings of a January 2004 review at the Oak Ridge Reservation, where we found that: (1) a performance test at Y-12 was compromised as a result of certain protective force personnel being allowed to view computer simulations of the test scenarios prior to the test; and (2) there was a pattern of actions by Reservation security personnel going back to the mid-1980's that may have negatively affected the reliability of site performance tests.

The Department's Unclassified Cyber Security Program

In Fiscal Year 2004, the Department spent about $2.6 billion on information technology to support its various missions. As required by the *Federal Information Security Management Act*, the Office of Inspector General conducts an annual independent

evaluation to determine whether the Department's unclassified cyber security program adequately protected data and information systems.

In our September 2004 report on cyber security, "The Department's Unclassified Cyber Security Program - 2004" (DOE/IG-0662), we found that the Department had initiated new policies that emphasized a risk-based approach to managing security that, when fully implemented, should strengthen cyber security across the Department. While these actions were commendable, problems continued to exist that could expose critical systems to compromise. Specifically, the Department had not:

- Completed certification and accreditation of each major system, to identify and mitigate risks;
- Prepared contingency plans to ensure that mission critical systems could continue or resume operations in the event of an emergency or disaster; and
- Taken action to ensure adequate security controls were in place at all sites.

Management concurred with our recommendations and informed us it is conducting a follow-on review of the Department's unclassified cyber security program.

Management of Oak Ridge Radio Projects

Department of Energy sites rely heavily on radio communications to support activities such as site emergency response, physical security, and protection. In its July 2005 draft report on the readiness of the Department's protective forces, the Government

Accountability Office stated that protective force officers at each of the five sites it visited reported problems with their radio communication systems.

In a June 2004 Office of Inspector General report on management of Oak Ridge Reservation radio projects, we identified that the two local Department of Energy management offices, the Oak Ridge Office and the Y-12 Site Office, were developing separate radio communication projects. We found that the two projects, as designed, would have created gaps in radio coverage and prevented Y-12 protective forces from maintaining communications with the rest of the Reservation and their own dispatcher in the event of an emergency.

In response to the report, management informed us that work on the separate radio system for the Y-12 Complex had been suspended.

These findings were similar to an earlier review at four other Department sites. During that review, we found that three of the four sites did not have direct radio communications with local law enforcement agencies that would have been called upon to assist in the pursuit of suspected felons or terrorists fleeing Department sites.

Implementation of the Design Basis Threat

The Office of Inspector General has undertaken a three-step process to review the Department's security programs and its progress in meeting the threat posed in the

revised Design Basis Threat (DBT) document. The DBT identifies the potential security threats to Department assets. As a first component in this strategy, we will be completing a review in the near future to determine whether the Department's National Nuclear Security Administration sites will implement the revised DBT by the end of Fiscal Year 2006. We will shortly be initiating a review to determine whether the Department's energy, science, and environment sites will meet the same requirement. As a third component to this process, we intend to review security initiatives throughout the Department to determine if all sites will meet the requirements of a subsequent revision to the DBT by the scheduled date of the end of Fiscal Year 2008.

Conclusion

The Department is addressing many security concerns and is doing so at substantial cost. We are concerned that, in a time of severe budget constraints, escalating security costs may force reduced expenditures for mission-related projects and programs. My office will continue to examine the Department's security apparatus, with the goal of providing recommendations to enhance efficiency and effectiveness.

Mr. Chairman and members of the Subcommittee, this concludes my statement. I will be pleased to answer any questions.

Mr. TURNER. Thank you.
Mr. Podonsky.

STATEMENT OF GLENN S. PODONSKY

Mr. PODONSKY. Thank you, Mr. Chairman, members of the subcommittee. Thank you for inviting me to testify regarding the readiness of protective force to defend Office of Energy, Science and Environment facilities in light of the GAO's recent report on their examination of protective force training and equipment at five ESE sites.

I will highlight relevant aspects of the GAO report from the perspective of the Office of Independent Oversight within my Office of Security and Safety Performance Assurance. These issues are addressed in greater detail in my written statement.

The Department considers its responsibilities to protect national security assets in our custody to be crucial. Secretary Bodman and Deputy Secretary Sell have demonstrated an intense interest and strong support for our security programs, and have continued the significant initiatives begun by their predecessors. This support includes the policy of holding line managers responsible for security program implementation and effectiveness, to include achieving established milestones for meeting the requirements of the Department's design basis threat.

While ESE site missions are generally associated with basic and applied scientific research and environmental remediation, rather than with national security matters, some ESE sites and, in particular, the five sites addressed in the GAO report—currently possess significant quantities of special nuclear material.

We agree with the GAO's general conclusion that protective forces at ESE facilities visited are adequately trained and equipped to protect the facilities under the current requirements. But there are some weaknesses that must be addressed.

This conclusion is consistent with our own previous independent oversight inspections of these facilities. We believe that ESE line managers and security professionals at all ESE organizational levels will move quickly and effectively to address the protective force training and equipment shortcomings outlined by the GAO, and will likely respond positively to recommendations contained in the draft report.

We anticipate efforts to do so will be integrated with many other actions necessary to meet the requirements of the design basis threat. We are confident that the new Under Secretary, Dave Garman, together with the newly appointed ESE Director of Security, Bob Walsh, will provide the immediate and sustained high level of attention necessary for these efforts to be successful.

We are currently pursuing a number of Department-wide initiatives designed to assist ESE in meeting its security challenges and obligations. Two, in particular are aimed at achieving affordable security upgrades to meet the design basis threat requirements. One of these is the Elite Force Initiative, by which we intend to enhance the tactical capabilities of those protective elements responsible for protecting our most critical national security assets.

We believe that to effectively defeat current and future threats, we need protective force elements possessing the advanced train-

ing, weapons, equipment, and tactics that will enable them to conduct a coordinated and intense offensive and defensive tactical operation at skill levels comparable to those of elite military units.

While achieving this goal will require some modified training and some upgraded equipment, together with policy changes, it should not require significant changes in manpower levels. Many of our current special response team personnel already possess high levels of tactical skills and are well armed and equipped. And this initiative is more about changing how we use some protective force resources than it is about adding more resources.

Further, this initiative will not directly involve protective forces at all ESE sites, especially those that do not possess critical national security assets, and may involve only a portion of the forces at sites protecting such assets. We have a number of activities under way to determine required changes in policy, defensive strategy and tactics, training, weapons, equipment, and supporting technologies that will enable us to effectively implement the elite force concept as envisioned on schedule.

Intertwined with the Elite Force Initiative is another complementary initiative, involving the increased use of security technologies to effectively and efficiently upgrade our protection systems. Through the prudent application of appropriate technologies, we expect increased use of those security technologies to provide cost savings and improved effectiveness over manpower intensive alternatives.

It is important to clarify that when we refer to security technologies, we do not refer exclusively to expensive, high technology and delicate electronic sensors. While such devices are certainly included, security technologies also include many other categories of items, such as improved barrier systems, materials that provide ballistic protection, advanced protective force weapons and equipment, and improved construction techniques. We expect the security technologies initiative to benefit all of our facilities.

The application of appropriate security technologies can improve effectiveness and efficiency of any protection system. Therefore, we believe all ESE sites are candidates for security technology upgrades, although we would expect more intensive investment in the benefits of such technologies at sites protecting our more critical assets.

I wish to note that the Idaho site within ESE has actually been extremely proactive with our security technology deployment initiatives and has recently submitted an impressive design basis threat implementation plan.

Through our technology deployment program, our site assistance visit effort, and our development activities, we are making progress in identifying and evaluating new technologies for site-specific applications.

In summary, Mr. Chairman and members of the committee, we agree with the general results, conclusions, and recommendations of the GAO report, and believe that ESE line managers under the new ESE leadership will address the issues identified by the GAO and the IG as they address the challenges associated with implementing the design basis threat.

We believe that our elite force, security technology, and other security initiatives will assist ESE meeting those challenges within the parameters established by Secretary Bodman and Deputy Secretary Sell. But they are challenges, and the ultimate success of the effort will in fact require the attention and support of ESE line managers at every level.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Podonsky follows:]

Testimony 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

July 26, 2005

Mr. Chairman and members of the subcommittee, thank you for inviting me to testify today as you assess the readiness of protective forces at DOE sites that are managed by the Office of Energy, Science, and Environment (ESE) in response to the GAO draft report "*Nuclear Security: DOE's Office of Energy, Science and Environment Needs To Take Prompt, Coordinated Action to Meet the Design Basis Threat*." I will address various aspects and implications of the GAO draft report from the perspective of the Office of Independent Oversight within the Office of Security and Safety Performance Assurance.

There is no more important responsibility for the Department of Energy than the safety and security of its employees and the communities around our facilities together with the protection of the vital national security assets in its custody. Secretary Bodman and Deputy Secretary Sell have acknowledged this, and have demonstrated keen interest in and strong support for our safety and security programs, and have continued the security initiatives begun by their predecessors. A vital element in the success of our protection strategy is holding line managers accountable for security program implementation and for meeting the established deadlines for implementing the requirements of the current Design Basis Threat policy. Due to the nature of its mission and the magnitude of its national security assets, the National Nuclear Security Administration (NNSA) is usually in the spotlight when it comes to security matters. However,

ESE sites – and in particular the sites addressed in the GAO draft report – currently possess and will continue to possess significant quantities of Special Nuclear Material that require protection equal to that afforded NNSA sites. The Department and its senior managers are responsible for providing effective protection for all national security assets in our possession, and to base that protection on the requirements of our Design Basis Threat policy and all associated needs, risks, and consequences – regardless of which Departmental organization has custody of the particular asset.

The subcommittee has expressed interest in three specific issues reflected in the GAO draft report: the status and adequacy of protective force training and equipment; the adequacy of resources provided to implement the requirements of the Design Basis Threat policy; and the coordination of security efforts across ESE sites. I will address those portions of the GAO draft report and the ESE security posture that fall within the scope of responsibilities of the Office of Security and Safety Performance Assurance. First, however, the GAO draft report addresses the protection capability of ESE sites in the context of the October 2004 Design Basis Threat policy. Let me bring you up to date on the status of the Design Basis Threat.

The current (October 2004) Design Basis Threat policy identifies an adversary capability that is significantly greater than that identified by previous the Design Basis Threat policy. In particular, the size of an adversary force that must be successfully countered was significantly increased. The magnitude of this increase caused some to question whether the new numbers were fully justified by the underlying intelligence estimates. In part to address these doubts, and to assure that the Department moves aggressively to plan and implement protection system

strategies in response to the requirements of the Design Basis Threat, Deputy Secretary Sell directed that the annual full review of the Design Basis Threat policy be conducted early, and be completed by July 1, 2005. At the same time, he directed that the October 2004 Design Basis Threat policy remain in effect, and that all requirements and associated milestones toward implementation would be enforced while the policy was being reviewed. The intelligence analysis completed as part of that review is now being validated by other appropriate executive agencies, to include the National Counterterrorism Center and we anticipate having interagency comments at the end of July. However, the Review has had no impact on NNSA and ESE efforts to develop and submit their Design Basis Threat implementation plans that are due July 29 which SSA is in the process of reviewing.

Before I address the contents of the GAO draft report, let me give you some impressions of ESE security efforts from the perspective of the Office of Security and Safety Performance Assurance. The missions of ESE facilities are generally not national security-related, and many, if not most, of their programs do not involve classified information or significant quantities of Special Nuclear Material. Their missions involve basic and applied scientific research as well as environmental remediation of former weapons complex facilities. Some of the environmental remediation facilities are not expected to be enduring, and security interests at those facilities will be gone or greatly reduced when the remediation work is complete. Understandably, ESE is especially cautious about investing the significant resources required to upgrade protection programs in response to the current Design Basis Threat at facilities that have limited or non-enduring security interests. However, in the Department's view, existing national security assets must be effectively protected as long as they are on hand. Further, ESE has a number of sites –

such as the Savannah River Site, Oak Ridge National Laboratory, Idaho National Laboratory, and the Hanford Site – that are expected to retain significant quantities of Special Nuclear Material for extended periods and which are in need of upgraded protection systems. We have seen some improvements in the ESE planning and implementation of security upgrades at its facilities and we have witnessed a new enthusiasm among some ESE managers. For example, our recent collaborative Site Assistance Visit effort, which I will discuss later in this testimony, included all but one of the ESE sites addressed in the GAO draft report – one of them (ORNL) at the express request of ESE. ESE has requested a similar visit to the remaining site (Hanford), and that visit is tentatively scheduled for September. ESE and its sites are in the process of developing implementation plans to meet the Design Basis Threat policy, and we will shortly see their formal proposals for security upgrades. ESE has been cautious with some of the Department's current security initiatives, and the need to move aggressively to implement upgrades when compared to NNSA, which admittedly has a much greater variety and concentration of vital national security assets than ESE. The uncertainty (due to schedule or project viability) of some of the ESE projects, such as the down blending of U-233 at ORNL and the removal of nuclear materials from Hanford, is influencing, at least in part, decision-making and progress. However, the Idaho site has moved out aggressively with a very impressive Design Basis Threat implementation plan and they have also enthusiastically embraced the application of new technologies in their security planning.

Comments on GAO Draft Report Conclusions

Now I'd like to address some of the specifics of the GAO draft report. First, GAO generally concluded that the protective forces at the ESE facilities visited are adequately trained and equipped to protect their facilities, but that they demonstrate some weaknesses that must be addressed. We agree with this assessment. There are no surprises here. This conclusion is consistent with our own previous safeguards and security evaluations of these facilities conducted by the Office of Independent Oversight and Performance Assurance. In fact, even the nature of the specific shortcomings called out by GAO, such as problems with radio communications coverage, are consistent with our past observations around the complex, including at ESE sites. GAO also acknowledged that the sites were aware of the identified shortcomings and were working to fix some of them. We also agree that the sites need to address the identified training and equipment deficiencies as soon as practical, and not wait until 2008, the date for full compliance with the current Design Basis Threat policy. Other issues identified as shortcomings by the GAO, such as individual participation in force-on-force exercises and the records tracking such participation, are more global in nature and will need to be addressed in Department-wide policy requirements. For this reason I have directed the Office of Security to revise the Department's protective force policies. The revisions are due to be promulgated by the end of this calendar year. We recognize that the GAO's conclusions regarding the current ability of ESE protective forces are based on current training and equipment requirements. As the Department and the sites implement plans to mitigate the Design Basis Threat, some protective force training and equipment requirements will evolve, and in many cases they are expected to result in increased requirements. However, our planning and

implementation process is intended to ensure that effective protection levels are maintained at all times.

We also agree with the GAO's conclusions supporting broader and more general actions required of DOE and ESE in order to meet the October 2008 goal for full implementation of the Design Basis Threat requirements. The GAO acknowledges the value of three major DOE security initiatives, and adds a fourth recommendation of its own. The GAO draft report essentially endorses three key elements of DOE's effort to upgrade its protection posture for significant quantities of Special Nuclear Material. These include creation of an elite protective force, introduction of new and additional security technologies to assist the protective forces, and consolidation of nuc lear materials to reduce the number of targets and locations that require the highest level of protection. To their endorsement of these initiatives, GAO adds a recommendation that ESE establish a security organization to manage these security efforts within ESE. We are encouraged by GAO's support of our own ongoing security initiatives. We also endorse GAO's recommendation to establish an ESE security organization. As it is up to the Under Secretary to determine the best way to manage ESE, we believe that an appropriate security organization at the highest level within ESE and with appropriate authorities delegated could facilitate effective and efficient management of security resources and implementation of required upgrades. Security upgrades will involve a substantial effort over the next two years, and if ESE is to achieve protection upgrade goals by October 2008, this sizeable effort must be well coordinated and well managed and fully endorsed by the Under Secretary for ESE.

While we largely agree with the conclusions and recommendations contained in the GAO draft report, we strongly disagree with GAO's expressed pessimism regarding our ability to implement our security initiatives on schedule. We take particular exception to this view regarding two initiatives identified in the draft report for which the Office of Security and Safety Performance Assurance has some direct responsibility: the elite force initiative and the security technology initiative. These security initiatives are not mere paper projects. We have been working on them for over a year now, and we are making substantial progress. More importantly, I see us continuing to emphasize improvements in these two key areas long after initial implementation is reached in 2008. We believe it would be of value to the members of the subcommittee to understand what these initiatives are, where we stand on them, and how they will affect security at ESE facilities.

The Elite Force

Let me first briefly clarify the scope of the elite force as we envision it. We recognize that to ensure success under current threat conditions certain segments of our protective forces must be able to employ coordinated and intense defensive and offensive tactical maneuvers with a high degree of skill and precision. The elite force will not be "modeled" after our military special forces as implied in the GAO draft report, because the elite force mission will be significantly different from that of military special operations units. However, the tactical skill levels required of our elite force are intended to be comparable to the skill levels of elite military units. We do not envision that all of our protective forces will require these elite skills. These advanced tactical skills and capabilities will be employed only to protect our most critical national security

assets, such as significant quantities of Special Nuclear Material. Sites that do not possess these vital assets – such as some ESE sites not included in the GAO review – will not be required to field an elite force. Requirements for protective forces at such sites will not change drastically, although addressing the current Design Basis Threat policy will certainly involve some improvements in skills, training, and equipment. Sites, under both NNSA and ESE, which possess critical assets, will be required to maintain an elite force whose primary responsibility is the protection of those assets. However, a site's entire protective force may not need to possess the elite-level capability – only that portion of the force directly responsible for protecting the critical assets. The elite force concept involves changing mission, organizational structure, and tactical methods of engagement as much as it involves increasing tactical skills. Many of our highly trained Special Response Team members already possess many of the skills that will be required of the elite force. Some of our elite force goals may be achieved through the redirection of existing resources. Therefore, the cost of implementing our elite force concept, while substantial, is not as extensive as one might imagine. The elite force will not be at all sites or engage all protective force members, and many of those protective force members who will be included already possess advanced tactical skills.

Let me summarize some of the significant steps we have taken so far in our efforts to define and implement the elite force concept:

- A Protective Force Working Group, with representation from my organization, NNSA, and ESE, spent many months defining and refining the elite force concept, analyzing alternative models, and selecting a preferred option for an elite protective force structure. The group also

identified changes in policy, training, and equipment that will be necessary to create the elite force. The group prepared a report of their activities and recommendations which was reviewed and approved by Ambassador Brooks and me and delivered to the Deputy Secretary on October 25, 2004.

- The Site Assistance Visit effort, conducted between November 2004 and April 2005, yielded important information regarding effective protection strategies and tactical options that will influence ongoing development and implementation of the elite force concept.

- In early January 2005 the Deputy Secretary directed implementation of actions to create the elite force. In late January, we assigned responsibility for continuation of the elite force implementation effort to the Office of Security and directed them to develop an implementation plan.

- In mid-May, we initiated that portion of the elite force implementation plan which could be implemented within SSA, namely: reviewing and drafting changes to DOE directives; developing enhanced training programs; and conducting follow-up inspections and validation activities.

- We have formally tasked the Office of Security and the Office of Independent Oversight and Performance Assurance with various responsibilities for implementing the elite force plan. The Office of Security created the Force Management Advisory Team to oversee further development of the elite force, with participation from NNSA, ESE, and the Office of Independent Oversight and Performance Assurance.

- Policy changes to support elite force objectives are being developed in parallel with the publication of streamlined policy documents.

- The DOE National Training Center, in Albuquerque, NM, is a key component to the improvement of the security and safety posture of the DOE and is developing new courses to support tactical leadership training, enhanced performance testing, and team tactical exercise programs. In November 2004, we designated the National Training Center as the Center of Excellence for Safety and Security Professional Development for the Department of Energy to serve as the Department's principle career development and training center.

- Draft language prohibiting protective force work stoppages has been developed and submitted with a recommendation that it be included in a revision to 48 CFR 952.204-2, the DEAR contract "Security Clause," that is being prepared for rulemaking.

- Subject matter experts at the Pantex plant are preparing to evaluate the proposed Physical Fitness Qualification Courses, which will be conducted under the auspices of the Texas Tech Institutional Review Board. The objective is to establish and validate the appropriate medical and physical fitness standards that would be used to determine a person's capability to complete the courses successfully. All events on the courses are tied to tasks required of protective force personnel, both routine and in response to security incidents. No special task accommodations will be required to support the elite force concept; however, qualification standards may be raised for elite force personnel, such as reduced qualification times for course completion.

- A task team met at Oak Ridge (Y-12), June 14-16, to initiate the development of elite force tactical doctrine and position classification, training, and response expectations within the parameters established by current regulatory directives.

- In mid-July we conducted a workshop at the DOE National Training Center. Participants included members of the Force Management Advisory Team, the Firearms Working Group, the Special Response Team Working Group, and members of the DOE protective force safety community. The agenda addressed: force structure; job analyses; elite force individual and team standards; deadly force rules of engagement; tactical doctrine and training methodologies; tactical deployment and response; weaponry, including firearms training, qualification, and employment; individual and team equipment; reconciliation of safety with realistic training requirements; technological augmentation of the force; review and development of policy revisions; and review of the regulations for possible revisions.

- Some sites, such as Savannah River, Hanford, and Y-12, have begun implementation of actions necessary to transition to an elite force by reorganizing their forces, revising response plans, and reviewing their training programs.

- A number of draft policy revisions to the streamlined *Safeguards and Security Program Planning and Management*, *Physical Security*, and *Protective Force* manuals have been completed and were discussed at the July NTC Workshop. The goal for publication of Departmental policy revisions affecting an elite force is December 31, 2005. We believe that we can implement the necessary elite force requirements within the scope of the current regulations.

Although we may need to amend some regulations in the future, implementation of the elite force will initially be accomplished through the Departmental directives process. For example, protective force arming, arrest, and use of force policies as promulgated by Title 10 Code of Federal Regulations Parts 1047 and 1049 were analyzed and identified issues were discussed with the DOE Office of General Counsel. Based on these discussions, we believe rule changes are unnecessary and that the identified issues can be addressed through policy and effective implementation of those policies.

As indicated by the above list of activities, there are many interrelated facets to implementing the elite force concept, and we are making progress in all areas. We expect to have a substantially upgraded protective force trained to higher standards, emphasizing tactical skills, in place by the end of FY 2008.

Security Technologies

Now let me update you regarding our position on security technologies and what we are doing to make better use of such technologies. We strongly believe that the expanded use of security technologies will allow us to increase the effectiveness and efficiency of our protection systems. Many technologies can serve as force multipliers to assist protective forces in accomplishing their missions more effectively and with less personal risk. The appropriate application of security technologies can enable fewer protective force personnel to meet the protection mission with reduced exposure to direct adversary actions, resulting in more effective protection systems and, in the long run, more cost-effective systems as well. The use of the term "new security

technologies" encompasses a wide range of devices from the highly sophisticated to the fairly simple and basic. Not only do these technologies include sensors and other electronic devices, but also various types of physical barriers, construction enhancements, protective force weapons, armored vehicles, and other types of equipment. These technologies also run the gamut in terms of costs and lead-times required to procure, install, and operate them. While the Department has always been active in identifying, and in some cases developing security technologies, we are now pursuing those efforts with greater intensity; and much of our activity involves ESE sites.

Last year we established the Center of Excellence for Technology Deployment at Pacific Northwest National Laboratory in Richland, Washington. The Center's mission is to seek out and evaluate new and recently developed security-related technologies and to facilitate the rapid deployment of appropriate technologies to serve as force multipliers or to otherwise improve the effectiveness and efficiency of our protection systems. The center has developed Memorandums of Agreement with two ESE sites – Idaho National Laboratory and Oak Ridge National Laboratory – to deploy a variety of new technologies prior to FY 2008 and beyond.

From November of last year through April of this year we conducted a series of collaborative Design Basis Threat Site Assistance Visits at DOE sites (including three ESE sites) expected to possess significant quantities of Special Nuclear Material on an enduring basis. The purpose of the visits was to work with local DOE and site personnel to identify alternate protection system designs, security technology applications, and protective force tactics that represent opportunities to contain protection system costs while providing an effective defense against the threat described in the October 2004 Design Basis Threat policy. Using a consistent approach and

methodology at each site visited, the collaborative teams consisting of security, technology, and tactics experts from my organization, NNSA, and ESE identified technologies and other innovations that could be employed to effectively and efficiently meet the Design Basis Threat policy. Following these visits, security experts at each site conducted formal vulnerability assessments to determine the specific technologies and other improvements they would employ in their upgraded protection system designs. A similar visit to the fourth and final ESE site possessing significant quantities of Special Nuclear Material is scheduled to take place in September.

Let me describe a few examples of the new technologies that, with ESE's cooperation and participation, we are already introducing to ESE sites to help them improve their protection postures. Unmanned Aerial Vehicles (UAVs) are being tested for future deployment at a large ESE site to help conduct surveillance of the vast areas inside the site's perimeter. The UAVs will be cued by fixed ground-based sensors that can detect an adversary at ranges sufficient to deny the ability to clandestinely stage attackers and equipment to enable an attack at a time that is advantageous to the adversary. The main objective is to use the information provided by the UAVs to enable the protective force to intercept and/or engage the adversary as far away as possible from the site's potential target areas. The UAVs will also be used to improve combat situational awareness by communicating information such as the adversary's strength and location to protective force responders should the site come under attack. As indicated above, we currently envision that the UAVs will be used in conjunction with other early warning sensors, such as unattended ground sensors, to provide a blanket of intrusion detection coverage in areas that cannot normally be observed by site personnel. One such system, developed by the

Department of Defense, uses a thermal camera to scan large areas at distances of several kilometers. The system, known as the Stabilized Panoramic Intrusion Detection and Recognition system, or SPIDER system, provides an alarm when a human enters the area that it is programmed to scan. This technology was shown to provide considerable benefit at an ESE site during a Site Assistance Visit by helping the responding forces to engage the adversary more quickly.

One of the threats seen almost every day in the news is the large vehicle bomb. Our Site Assistance Visits have shown that in some cases a vehicle bomb would have a potentially devastating effect on site security and expedite the adversary's ability to enter a target facility and recover Special Nuclear Material. We have worked with ESE sites to help them develop an overall protection strategy for explosive threats, including vehicle bombs. We have also facilitated the installation of a new type of affordable vehicle barrier at several NNSA sites, which significantly enhances their ability to mitigate this threat at a much lower cost per linear foot than previous designs. What makes this barrier unique is its ease of installation and its ability to effectively stop very large vehicles moving at highway speeds. This barrier and the lessons learned at the NNSA sites have been recommended for use at ESE sites where vehicle bombs are considered attractive methods for attackers.

We have deployed the Advanced Concept Armored Vehicle (ACAV) with installed remotely operated weapons systems (ROWS) at two NNSA sites. We are also in the final stages of deploying multiple ROWS on the interior of an NNSA facility. This deployment application has served to integrate and demonstrate all of the security, safety, training, and administrative factors

needed for deployment. Lessons learned should help the expedited deployment of ROWS at other Departmental sites. These weapons present a formidable obstacle to the adversary, particularly when deployed with other activated systems. Not only do we expect them to improve our ability to neutralize adversaries, but they will also improve the survivability of our protective forces. Our future plans call for assisted targeting technologies to be integrated into these weapons. We anticipate this will eventually lead to manpower savings by allowing an operator to control more than one weapon. Several ESE sites are planning to deploy these weapons in both interior and exterior applications.

We are also investing in new non-lethal technologies which can reliably overwhelm an adversary who has made more progress toward a target than is desired. One example involves the use of directed energy technology previously developed by the Department of Defense for non-lethal applications. The technology uses millimeter wave energy to create an intolerable level of heat on a person's skin, effectively forcing the adversary to move to a different location to escape the weapon's beam. Our current focus is on a smaller and less expensive short-range version of the Department of Defense long-range system. We expect to make this technology available to ESE sites in 2008.

We are also investigating the use of certain commercial grade fire suppression systems as an innovative method of denying adversaries access to Special Nuclear Material. One such system can deploy an offensive gaseous substance very quickly, creating a very hostile environment for adversary operations. At least one ESE site is seriously considering deploying this technology based on the results of their Site Assistance Visit.

We are working with two ESE sites to deploy a system we have been investing in that is capable of tracking the location of protective force responders both inside and outside of buildings, and displaying this information to response force commanders. It also provides a duress capability and vital sign information about each individual responder. Understanding where our responding forces are located during a battle, and their state-of-health, can significantly improve the tactical effectiveness of our response force commanders and positively influence the outcome of a conflict.

These few examples of security technologies represent small individual capabilities that, when used collectively and integrated into protection systems, can have a synergistic effect that improves overall system effectiveness without significant increases in manpower. We are also evaluating and introducing various other technologies, including advanced armored response vehicles, anti-armor weaponry, and many others. We are confident that, with adequate resources, we can procure and integrate appropriate new security technologies into our protection systems within the timeframe established by the Secretary.

I also want to mention one other very important point that was only discussed briefly in the GAO report. GAO noted that a number of protective force members believed that safety constraints placed on their actions during force-on-force exercises greatly reduced the realism of the training provided. In concluding this short discussion of the initiatives to implement an elite protective force and to inject new technologies into our security planning, I must point out that safety constraints are encountered in almost every aspect of this effort, not just force-on-force

performance testing. This is not because safety and security are naturally at odds. Rather, we have to do a better job of coordinating safety and security analyses, assessments, and requirements to ensure we are satisfying both disciplines to the benefit of our protective force. SSA, NNSA, and ESE have recognized this need and have been discussing for some time a mechanism to achieve this important goal. While there is not yet a fully agreed-upon mechanism, the Department at the highest levels of management is working diligently to resolve this safety and security integration issue and has established a security/safety interface working group.

Concluding Remarks

Mr. Chairman and Members of the subcommittee, in summation let me reiterate that we concur with the general results, conclusions, and recommendations of the GAO draft report, which indicate that ESE protective forces are sufficiently trained and equipped to protect their sites, based on current expectations, but demonstrate some training and equipment weaknesses that must be addressed in order to meet the requirements of the October 2004 Design Basis Threat policy. Our own evaluations and observations support this conclusion. While a significant effort remains, we are confident that we can transition the appropriate protective force elements to elite force status over the next two years and be better prepared to counter the threat. I would also like to emphasize the seriousness with which the Department's senior managers, as well as other Departmental elements, are treating our efforts to implement necessary upgrades to our protection systems within established time frames. Although technology development, evaluation, and implementation is a continuous process that will occur as long as we have

protection systems, we are confident that we can integrate appropriate available technologies into our security posture over the next two years.

Accomplishing all this along with our other concurrent security initiatives is an ambitious undertaking. We have a lot of work to do; we can't afford to waste time and we can't afford to approach the challenges tentatively or half-heartedly. We will need the continued support of the Department's senior managers – which I firmly believe we have and will continue to have – and line managers, as well as support from Congress. We have the strong and committed support of Secretary Bodman and Deputy Secretary Sell. The Administrator, NNSA, has provided strong leadership over the recent years and is strongly supportive today. We look forward to the same support and leadership from the recently confirmed Under Secretary. ESE line managers at all levels must step up to the plate and demonstrate the full support necessary for protection system upgrade efforts to ensure that their sites are capable of protecting against the Design Basis Threat under the conditions established by the Secretary.

Thank you.

Mr. TURNER. Dr. Brede.

Also, I want to acknowledge that Carolyn Maloney has joined us.

Mrs. MALONEY. Thank you.

Mr. TURNER. Dr. Brede.

Dr. Brede, I don't think your mic is on.

STATEMENT OF DR. LAWRENCE BREDE

Dr. BREDE. Mr. Chairman and members of the subcommittee, thank you for the opportunity to appear before you today to offer my views on the readiness of Department of Energy Office of Energy, Science and Environment protective forces to meet the terrorist threats identified by the intelligence community.

The perspective I bring to the table is that of a senior contract manager for a protective force and a soldier. Until recently, I served as General Manager of the Savannah River site protective force contract, one of the five sites recently reviewed by the GAO. I served in that capacity for more than 12 years. And prior to my DOE service, I spent 26 years as an Army officer with three combat tours, including service with elite units.

Let me say up front, for the record, that our protective forces are well trained and, as a group, are as capable as any of the military units with which I have served. In fact, the majority of protective force officers with whom I am familiar come from a military background and bring with them the skills necessary for the protection of critical DOE assets.

Anecdotally, the winner of two annual recent National Level Tactical Competitions comes from a DOE ESE site. In these competitions, they scored consistently higher than military, law enforcement, and Federalized forces in tests of shooting, physical fitness, and tactical skills.

With reference to the GAO report, I believe it provides a balanced assessment of ESE protective force readiness to defend their respective sites. The report's conclusions, that protective forces generally meet existing key DOE readiness requirements and comply with DOE standards, firearms proficiency, physical fitness levels, and equipment standardization are accurate ones.

At the same time, the report's identification of possible weaknesses and actions needed to correct these could serve to enhance our abilities to defend against the 2004 design basis threat. Because it matters not how capable we are today, we ought to work at being better than we are. Our sites can and are addressing the weaknesses in training and equipment identified in the GAO draft report.

I would submit if the GAO would conduct a review today on force readiness at ESE sites, the results would be significantly different than the snapshot taken when the last review began in March 2004. Today's picture would reflect more tactically focused training, the employment of more advanced weapons systems, communications, and armored vehicles, and a host of other actions related to meeting the 2004 DBT.

Similarly, I believe that site contractors understand the necessity to take our protective force readiness and capabilities to the next level. That is, we need to transform certain segments of our legacy force to an elite force. Based on secretarial guidance and Office of

Security and Safety Performance Assurance initial efforts, some sites—and the Savannah River site among them—have already taken actions to transition to this elite force with challenging training, increased performance standards, and tactical reorganization.

I also believe that the transformation to an elite force can be facilitated by policy considerations in four areas: more challenging physical fitness qualification standards; introduction of height, weight, and body composition standards; identifying appropriate safety performance expectations; and considering a uniform retirement plan to allow for cycling of human capital through elite force units.

In conclusion, I believe that ESE protective forces are sufficiently trained and equipped to meet existing DOE readiness requirements. Site implementation plans identifying how sites will meet the increased challenges presented by the October 2004 DBT have been provided to DOE ESE and are being reviewed for approval. Meanwhile, my experience indicates we are being provided the resources necessary to support the phased implementation of measures to meet 2004 DBT protective force requirements.

While addressing certain policy issues will certainly enhance our force readiness, I have confidence in our protective forces' ability to counter today's and future threats. Simply stated, I am as proud to serve as these forces as I was to serve with America's sons and daughters in my military experience.

Thank you, Mr. Chairman.

[The prepared statement of Dr. Brede follows:]

TESTIMONY OF DR. LAWRENCE BREDE
SENIOR VICE PRESIDENT, DOE OPERATIONS
WACKENHUT SERVICES, INCORPORATED
FOR THE HOUSE SUBCOMMITTEE ON NATIONAL SECURITY,
EMERGING THREATS, AND INTERNATIONAL RELATIONS
JULY 26, 2005

Mr. Chairman and Subcommittee Members,

Thank you for the opportunity to offer my views on whether Department of Energy Office of Energy, Science and Environment (DOE/ESE) protective forces are sufficiently trained and equipped to meet the terrorist threats identified by the intelligence community. Additionally, I have been invited to provide a contractor's assessment of whether DOE/ESE is providing adequate resources for implementation of measures to deal with the 2004 Design Basis Threat (DBT).

To provide some context for my perspectives, it should be noted that my views are shaped by my 14 years experience as a DOE protective force manager, and 26 years as an Army officer. Until recently, I served as Senior Vice President and General Manager, Wackenhut Services, Inc. – Savannah River Site (SRS), one of the five sites reviewed in the GAO DRAFT report (GAO-05-611), *Nuclear Security: DOE's Office of Energy, Science and Environment Needs To Take Prompt, Coordinated Action to Meet the New Design Basis Threat.* I served for more than 12 years in that position and came to SRS from the Department of Energy's Pantex Plant where I served briefly as the Protective Force Manager. My 26 years in the Army included service in three armed conflicts -- Vietnam, Operation Just Cause in Panama, and Operation Desert Storm in Iraq. I commanded an elite military force during the last two combat tours.

My invitation to testify requested that I focus my testimony on the previously mentioned GAO Draft report. Essentially, the report provides a thorough review of DOE protective force preparedness and offers a balanced assessment of their readiness to defend DOE sites. The report's conclusions that protective forces "generally meet existing key DOE readiness requirements" and "comply with DOE standards for firearms proficiency, physical fitness levels, and equipment standardization" are accurate ones. The GAO team's approach to identify possible weaknesses which, if corrected, could enhance our protective forces' ability to defend against the 2004 DBT is a valid one.

Let me say up front, for the record, that our protective forces are well-trained, as groups are as capable as any of the military forces with which I have served, and are motivated to further hone their tactical skills. In fact, the majority of protective force officers with

whom I am familiar come from a military or law enforcement background and bring with them the skills that are necessary for the protection of our national security. Anecdotally, the winner of two recent national-level tactical competitions comes from a DOE/ESE site. In these competitions, they scored consistently higher than military, law enforcement and federalized forces in tests of shooting, physical fitness and tactical skills.

Given that as a backdrop for my testimony, I would note that no matter how capable we might be today, we ought to work to be better than we are. To that end, I offer my views on four areas addressed in the GAO draft report: training, the conduct of force-on-force exercises, equipment, and transformation to an "elite force."

TRAINING

The report notes that most protective force officers (74 of 105) "are not at all confident in their current ability to defeat the new threats contained in the 2004 DBT." In fact, there is no expectation that today's protective force will absolutely prevail against the more substantial 2004 DBT until implementation is completed at the end of FY 2008. Nevertheless, these officers and their leaders are trained, motivated and capable of protecting DOE assets against the adversary force they have been trained to defeat.

The report also notes that a very large fraction of officers interviewed (85 of 105) identified deficiencies with their training, especially regarding the "frequency and quality of firearms and tactical training." However, a review of training records by the GAO team indicated that the majority of officers (79) met their weapons qualification requirements within the required time period and an additional 8 officers met their requirements shortly thereafter, due primarily to the closure of a site's firing range during an incident investigation. While additional training is certainly more desirable, the current duration and frequency of live-fire training provides our officers the skills necessary to successfully engage adversaries. For example, the SPO II's at SRS not only undergo 16 hours of firearms qualification training per year (8 hours each, semi-annually), but an additional 16 hours of live-fire training involving Situational Training Exercises (STX's). This quality training includes lateral and diagonal tactical movement through tactical lanes, two-officer fire team training, downed officer rescue, wearing the protective mask while engaging targets with both rifles and handguns, both daylight and low-light shooting and obstacle negotiation among other various firearms skill tests. Our SPO III's (special response team members) receive significantly more firearms training than noted here. In short, our officers receive their required semi-annual qualification training, but also "above-the-line" live-fire training that requires them to shoot on the move as fire teams in challenging situations.

Perceived shortfalls in the frequency and quality of tactical training, apart from firearms training, are being overcome. A recommendation by the Office of Security and Safety Performance Assurance (SSA), supported by ESE, was made in August 2004 to "eliminate the remaining vestiges of the old industrial security/law enforcement Protective Force model and replace them with a military base defense model, supported by appropriate unit organization and training." Since that time, sites have been

aggressively pursuing tactical training and SSA is testing against tactical standards in their field assessments. At SRS, for example, all SPO II's receive a total of 30 hours of tactical training (in addition to live fire training) and those SPO's assigned to sensitive facilities will receive 105 hours of tactical training in FY 06. Such training includes team training in shooting, moving and communicating; employing modern training technologies such as man-on-man engagements with dye-marking cartridges and Engagement Simulation System lasers; employment of optical aids such as thermal imaging and advanced rifle scopes; night-fighting, recapture operations; and donning and fighting in chemical and biological personal protection equipment. Officers report that they are challenged and highly motivated by such training and there are noticeable improvements in individual and unit skills.

FORCE-ON-FORCE EXERCISES

Force-on-force exercises are the crucible for protective force training. They test individual and team tactical skills, command and control capabilities, communications, and total systems effectiveness. Consequently, these exercises are the best test of force readiness. At the same time, these are substantial undertakings because they are expensive ($15 – 80K per iteration, depending on the complexity of the facility/system being tested), require months of planning, and present potential safety hazards.

The GAO report identified two issues associated with force-on-force exercises:

1) Only 46 of 84 protective force officers who had participated in such exercises believed that they were either realistic or somewhat realistic.
2) DOE does not have a requirement for individual officers to participate in these exercises, nor is there a requirement that sites track individual officers' participation.

With regard to the realism of force-on-force exercises, some clarification is required as to what the surveyed officers meant. For the 38 officers who believed that force-on-force exercises were not realistic, were they of the opinion that these exercises were overly conservative (i.e. the adversaries demonstrated less of a capability than could realistically be expected), or that the adversaries' capabilities were so substantial as to not be credible?

Relatedly, the GAO team found that 33 of 84 officers reported that safety considerations interfered with the realism of the exercises because they were limited in the tactics they could employ (e.g., exceeding the speed limit in patrol vehicles, not climbing fences, or not being able to run in certain areas). To some degree, these officers' perceptions are correct. Typically, "safety walk downs" are conducted in an exercise area prior to the conduct of an exercise to identify potential hazards to participants. Subsequently, control measures are identified and implemented to reduce the probability of injury or even death. Therefore, the realistic conduct of an exercise may be somewhat attenuated by these precautions. What may be shaping our officers' perceptions is the appearance of safety personnel having veto authority over security planning. What DOE/ESE and

protective force managers must ensure is that there is a balance between safety and security considerations when planning force-on-force exercises.

The second issue raised with regard to these exercises is the lack of a requirement for individual officer participation in major force-on-force exercises, or a requirement for sites to track such participation. This finding is accurate as there is no such policy requirement. Site security contractors do maintain training records for officer participation in individual training, but have not done so for individual officer participation in unit training during force-on-force exercises. DOE shares the GAO's concern about officer participation in force-on-force and other tactical training with some degree of regularity and is developing appropriate policy changes. As a practical matter, at least two of the five sites surveyed by the GAO now record protective force member participation in force-on-force exercises.

As DOE considers relevant policy changes, I would recommend that training records be maintained on team or unit participation in force-on-force exercises. As we work to build unit cohesion in an elite force (see later testimony), we should measure unit effectiveness in training. Military units maintain records on unit participation in major training exercises and their associated success or failure. As DOE protective forces have a paramilitary mission, we should adopt similar policies. In short, individual training records should reflect participation in *individual* training and unit training records should record the results of *unit* participation in major exercises.

EQUIPMENT

The GAO report concluded that the five ESE sites visited had the equipment necessary to "generally" meet the readiness requirements contained in DOE orders and federal regulations. They did, however, find some weaknesses that they believe could adversely affect the ability of ESE forces to defend their sites. Among these weaknesses were the lack of dependable communications systems; insufficient protective gear, including protective body armor and chemical protective gear; and the lack of armored vehicles.

Following the issuance of the 2004 DBT, the Office of Security and Safety Performance Assurance (SSA) initiated Site Assistance Visits (SAV's) to assist sites in meeting the increased requirements of the new postulated threats. Reportedly, four of the five ESE site examined by the GAO team received these visits. These substantive visits by SSA included subject matter experts who evaluated response plans in preparation for the new DBT, advised on the applicability of new and emerging security technologies, and offered equipment recommendations. Since that time, sites have modified equipment lists to better meet 2004 DBT challenges

Some of the equipment shortcomings cited in the GAO report are resource-driven and are in the process of being fixed with DBT funding based on priorities. At SRS, for example, some armored vehicles are on station with more to follow. They were not on site when the GAO team did their assessment. Advanced weapons systems have also been

procured and others are in the procurement system. Comments on other equipment issues follow:

Communications Equipment. The GAO report indicated that 66 of the 105 protective force officers reported that they did not always have dependable radio communications, with 23 officers identifying sporadic battery life and 29 officers reporting poor reception at some locations on site. Communication upgrades at one site now provide for higher capacity nickel metal hydride batteries in portable radios. Transitioning to state-of-the-art lighter, smaller portable radios has also resulted in a better service history. However, there are still a limited number of communication "dead spots" which cannot be technically overcome because of the nature of the structures in which Special Nuclear Material is stored. To overcome this problem, officers are trained on the location of these poor reception areas and alternate means of communication are made available to include hard-wired "ring down" phones and PA systems.

Individual Protective Gear. Protective gear, including protective body armor and chemical protective gear are absolute necessities for the threats our officers face not only under the 2004 DBT, but also under the current postulated threat. At the one site where most Security Police Officer II's had not been issued body armor and had received a waiver for that requirement, testing and procurement actions for body armor are now taking place. Equally important is the necessity for Security Police Officer II's to be able to fight in chemically contaminated environments. Security Police Officer III's at all surveyed sites were equipped to operate and fight in such environments, but all SPO II's were not. I certainly agree with the GAO team's conclusion that both protective masks and special protective suits be available to all officers who are expected to fight in chemically contaminated environments.

Armored Vehicles. The report notes that only a single ESE site, as opposed to all NNSA sites, with Category I Special Nuclear Materials has armored vehicles. The report also correctly notes that there is no DOE requirement for such vehicles. The DOE rationale for this policy is that armored vehicle use and employment must be tailored to the protection strategy for a particular facility. I agree with that approach. Armored vehicles are a mobile fighting platform which may or may not be appropriate for certain kinds of targets, and their employment should be based on a terrain analysis. At the Savannah River Site, no armored vehicles were available at the time of the GAO review, but are now on station.

TRANSFORMATION TO AN ELITE FORCE

Of the areas addressed in the GAO report, this effort may be the one with the greatest potential for enhancing protective force readiness and capabilities. The report notes that "to successfully defend against the much larger terrorist threat contained in the 2004 DBT by October 2008, DOE and ESE officials recognize that they need to take several prompt and coordinated actions," to include the transformation of current protective forces into an "elite force." The former Secretary of Energy proposed in May 2004 that this force be patterned after the U.S. military's special operations forces (e.g., Army

Rangers and Navy SEALS). These special operations forces have as their primary mission the destruction of targets through rapid deployment, stealth, and violent execution of operational orders. Conversely, protective forces have as their primary mission the defense of critical DOE assets. Therefore, it is now commonly understood that the Secretary meant that DOE protective forces ought to be as well-prepared to perform their mission (defense) as special operations forces are to perform theirs (destruction).

I would point out that "elite" forces already exist within the Department of Energy. Sites with SPO III's have forces which must meet increased standards for weapons qualification and fitness, receive increased tactical training, and are generally incorporated as the ultimate force option in response plans. Therefore, in my view, transforming existing forces to an "elite force" translates to raising the standards for SPO III's to an even higher level and enhancing the existing capabilities of SPO II's.

It should be noted that while this transformation is clearly desirable to provide a substantial defense and higher levels of confidence in defending DOE targets, current DBT implementation plans do not require the establishment of elite forces beyond additional numbers, training, and weaponry. Nevertheless, both DOE officials and contractor security managers have ongoing actions to improve the capabilities of our protective forces. The Office of Security and Safety Performance Assurance is currently defining the requirements for an elite force to protect DOE's most critical assets, and identifying the necessary policy changes to create and sustain such a force through a Force Management Advisory Team (FMAT). The FMAT is comprised of subject matter experts from throughout DOE and supporting contractor organizations. Similarly, contractor protective force managers have initiated efforts to increase tactical training and raise performance standards for protective forces at DOE/ESE sites.

Currently, protective force contractors are moving existing, or "legacy," forces to a more capable "interim" force with resources currently available. Understanding that we are moving away from an industrial /law enforcement protective force model to a military "base defense" model, training resources are being effectively redirected to improve the tactical capabilities of our forces. For example, we have been able to accomplish this at the Savannah River Site by increasing tactical training hours and instituting a training relief shift.

While substantive efforts are underway to move our legacy force to an interim force with enhanced tactical capabilities, there are certain policy and regulatory issues which must be dealt with to achieve the objective "elite" force. These follow:

Physical Fitness Standards. The level of physical fitness of a security force has a direct impact on the operational readiness and the ability of a unit to fight and win. Existing DOE protective force fitness and, relatedly, medical standards can be improved upon to support the creation of an elite force.

A military-type physical fitness test should be the standard by which individual readiness is measured for those forces designated as "elite" forces. For example, the Army Physical Fitness Test is a validated, three-event physical performance test that measures muscular endurance and cardio-respiratory fitness levels. It is easily administered, age- and gender-specific, and battle tested. This standard results from world–class research and analysis by physicians and fitness specialists who comprise the Army Physical Fitness Board. The type of rigor associated with elite force standards stresses the body in wear and tear and, hence, a graded scoring scale based on age and gender is appropriate for our purposes. Adoption of the Army standard, or one similar, would require little or no further analysis by DOE. Additionally, these standards are likely to be defensible if legally challenged because there is a precedent (the military), and there is no adverse impact on protected classes (primarily female protective force officers). While we are likely to hear arguments for a single standard (SPO's should be held to the same standard for the same job), adopting military standards to accomplish a paramilitary mission should be legally defensible. To accomplish this regulatory change, the Code of Federal Regulations would have to be modified to adopt military standards as the DOE fitness standard for those forces designated to protect selected categories of Special Nuclear Material.

Height and Weight Standards. DOE policy should incorporate height and weight standards for DOE protective forces to enhance operational readiness. Overweight SPO's simply do not have the wherewithal to conduct tough, demanding tactical training and are more prone to injury. Individuals with excessive body fat reflect a lack of personal and organizational discipline, and negatively influence organizational character and morale. A strong deterrent to an adversary force is the appearance of a tough, professional security force prepared to violently execute response plans.

To improve force capabilities, DOE should adopt a body composition program that includes height, weight, and body fat standards. Once again, the Army uses an age- and gender-specific height and weight screening table to delineate their standards. The Army accounts for differences in body composition (e.g., as with weightlifters) by allowing those over the screening weight table to have an allowable percentage of body fat. DOE could adopt a similar program to enhance force readiness.

Safety Performance Expectations. Protective force officer participation in rigorous training while routinely meeting challenging performance standards will require DOE/ESE to reassess safety performance expectations. Comparing protective force injury rates against those of site operating contractors will create an unfair, biased comparison. New DBT requirements necessitate the safe integration of state-of-the-art security and military technology into nuclear facility operations. New training programs to support remote weapons systems, explosive capabilities, and shoot-on-the-move tactical training courses are becoming a routine part of protective force training. The aggressive nature of elite force, tactically-biased training will require a new baseline of protective force safety performance expectations.

Elite forces in the U.S. military special operations community undergo tough, challenging training. Their accident and injury experience are more likely to be akin to elite protective force training than that of DOE site operating contractors. Benchmarking the safety performance of military special operations forces and training programs will likely provide reasonable baseline expectations for the DOE/ESE elite force.

Uniform Benefit and Retirement Plan. One of the most critical components in transforming the legacy force into an elite force is the ability to effectively cycle human capital. As physical standards and training requirements are raised, the ability to efficiently replace protective force officers who can no longer meet elevated standards will be a critical system feature. The military model offers a 20-year retirement with medical benefits to support the cycling of personnel through military units. The DOE will have to examine the potential for twenty-year and medical retirement benefits to provide for effective exit options for elite force personnel when they can no longer meet standards.

The military model promotes a strong sense of loyalty as foundational to its elite forces. That loyalty is established on the premise that the payoff for training hard, regularly demonstrating your capabilities, and standing ready to make the ultimate sacrifice is rewarded with a graceful way out for those who have served honorably. Absent such a mechanism, the elite force human capital cycle will develop a bottleneck of employees who do not have a viable "way out" and who can no longer meet tough standards. While there may be significantly increased costs associated with such a plan, DOE should consider the creation of a universal retirement and medical benefit plan that will promote the maintenance of an elite protective force.

CONCLUSIONS

DOE/ESE protective forces are sufficiently trained and equipped to meet existing DOE readiness requirements. Site implementation plans identifying how sites will meet the increased challenges presented by the October 2004 DBT are being provided to DOE/ESE by the end of July 2005. Meanwhile, the ESE site for which I had security responsibilities (Savannah River Site) is providing the necessary resources to support the phased implementation of measures to meet October 2004 DBT protective force requirements. Of course, funding for the out years must provide for adequate resourcing of requirements identified in the implementation plans.

The protective force training programs with which I am familiar have been well-planned, aggressive, and performance-oriented. Training and equipment shortfalls identified in the GAO DRAFT report (GAO-05-611), *Nuclear Security: DOE's Office of Energy, Science and Environment Needs To Take Prompt, Coordinated Action to Meet the New Design Basis Threat,* have been corrected or will be corrected in the near term.

The continued development of an elite force will do much to counter the increased threat addressed in the October 2004 Design Basis Threat. I am aware that the Office of Security and Safety Performance Assurance, supported by ESE, is currently working to

revise existing DOE protective force policies and practices to facilitate movement from an interim force to the objective elite force. In my view, the most pressing policy needs relate to:

- Physical fitness standards
- Height and weight standards
- Safety performance expectations, and
- A uniform benefit and retirement plan

While addressing these issues will clearly enhance our force readiness, I have confidence in our protective forces' ability to counter today's threat. Simply stated, I am as proud to serve with these forces as I was to serve with America's sons and daughters in my military experience.

Thank you, Mr. Chairman, for the opportunity to appear before this Subcommittee today and offer my views on DOE/ESE protective force readiness.

Very respectfully,

Lawrence Brede, D.P. A.
Senior Vice President and
Executive General Manager
Department of Energy Operations
Wackenhut Services, Inc.

Mr. TURNER. Dr. Adler.

STATEMENT OF DR. GLENN ADLER

Dr. ADLER. Mr. Chairman and members of the subcommittee, thank you for the opportunity to testify today. I am Glenn Adler, and I work for the Service Employees International Union. I have submitted a statement for the record and will summarize the main points.

We have three main concerns. The best standards in the world will not improve security if contractors elude them if DOE's oversight is weak, or if DOE lacks the will to weed out poor performers or to avoid choosing them in the first place in the procurement process.

SEIU is one of the largest trade unions in the United States, with more than 1.8 million members. We are the largest union of security officers in the country. I am responsible for coordinating research and policy work in the Federal sector, including in DOE nuclear facilities and NRC regulated commercial nuclear power plants.

On September 11th, our security officers and janitors at the World Trade Center, were among the first responders to that terrible tragedy, working side by side with the NYPD and the firefighters in a cause to which many of our members gave their lives. But well before the horrible events of September 11th, SEIU had been raising the issue of security standards, most notably for airport security screeners. We have partnered with responsible contractors, building owners, mayors, and Governors, to raise standards and improve performance.

We know DOE's regulations for training and performance are, as they should be, far beyond the standards in the commercial office world. But the GAO report, on the table today, tells us that contractors are in significant ways not living up to them. Consider one failure identified in the report and then echoed in the fine presentation by the Inspector General, undependable radio communications. This may sound like a minor matter to some people, but it may contribute to serious problems. In fact, one may have already occurred.

According to the New York Times, in 2004, poor radio communication played a role in the confusion of a near friendly fire incident at the Y–12 plant in Tennessee. Officers are courageous people, people doing difficult and important work. They are heavily armed, and they go out into the night and we learn that perhaps their radio communication doesn't allow them to talk to each other. To what extent is DOE's multibillion dollar security budget compromised by poor radios and dead batteries? A chain is only as strong as its weakest link.

This problem is directly connected to issues that are not directly addressed in the GAO's report, the oversight and accountability of contractors' behavior. SEIU believes security should be of the highest standard, whether performed by public authorities or by private companies. We are not opposed to privatization. But contractors' interest in the bottom line may encourage cheating and cutting corners.

In response, we expect government to check and balance their behavior, and to change the incentives that may lead to cutting of corners. But the Department sometimes contributes to these irresponsible outcomes. The GAO has consistently warned DOE about problems, for example, with their award fees. Yet, these problems persist today.

You are all familiar with last year's IG report on cheating by the foreign-owned contractor Wackenhut during a security drill at Y–12. The incident cost the contractor about $200,000 in fees. But the company still received a good performance grade from DOE and a $2.3 million award fee. Rather than a multimillion dollar award fee, such outrageous practices demanded serious sanctions from the DOE, including the consideration of canceling the contract, suspension, or debarment. Remember, this is cheating at a facility that contains special nuclear material.

We have heard from multiple security employees at other DOE ESE sites that these practices are not confirmed to Y–12. And some security officers told us the motto is "if you ain't cheating, you ain't competing."

Oversight exercised by the Inspector General is critical to corralling this sort of behavior, but their oversight has been subject to continuous public criticism by contractors. After the recent IG report on training problems at Oak Ridge, which is referenced in the GAO report and which was mentioned by the representative from the IG, a Wackenhut spokesman mocked the IG as "bean counters who didn't understand security practices." Such comments indicate contempt for the agencies, including Congress, to whom the IG reports, who are charged with oversight of these facilities. They create an impression, in the minds of the public, at least—at odds with expectations of oversight and accountability.

To us, the conditions described by the GAO report are shocking but not entirely surprising, since we encounter very similar problems in other contexts: NNSA sites, commercial nuclear power plants, and U.S. military bases. However, today's report and other GAO and IG investigations tend to mirror the structure of DOE itself, taking a piece of the puzzle and looking at it in depth.

We believe it is important to complement these perspectives by assessing the contractors, and not just the agencies, and looking at their entire record across different settings to learn whether a problem reported at one facility is an isolated event or part of a broader problem and pattern of poor performance. This will help in oversight of current contractors and, if applied during the procurement process, will help weed out poor performances before they are even awarded a contract.

In conclusion, the best standards in the world will not improve security if contractors elude them, if DOE's oversight is weak and if DOE lacks the will to get rid of poor performers or to avoid choosing them in the first place.

We make a few recommendations: One, that DOE urgency implements an effective process to monitor performance and weed out poor performers, rather than reward them; a review of award fees and the robust use of penalties to enforce compliance; DOE must have a dramatically lower tolerance for cheating and cutting corners, making it too expensive for a contractor to risk this kind of

behavior; and, faintly, DOE acquisition processes should be strengthened to ensure contracting officers do the proper due diligence by assessing security contractors' past performance and their record of business integrity and ethics. This is already in the Federal acquisition regulars, but is not always applied in practice.

Thank you very much, Mr. Chairman.

[The prepared statement of Dr. Adler follows:]

TESTIMONY of Dr. GLENN ADLER

Property Services Division
Service Employees International Union

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

July 26, 2005

Mr. Chairman, Ranking Member Kucinich, and members of the Subcommittee, thank you for the opportunity to testify before you today. My name is Glenn Adler, and I am a research analyst in the Property Services Division of the Service Employees International Union (SEIU).

We welcome this opportunity to testify before your committee, and appreciate Chairman Shays' leadership on this issue and for recognizing the value of talking with organized labor on a matter where security officers' workplace conditions, contractors' performance, DOE oversight, and national security intersect.

THE SERVICE EMPLOYEES INTERNATIONAL UNION

SEIU is one of the largest trade unions in the United States, with more than 1.8 million members. More than 50,000 private security officers and public safety personnel are members of SEIU. More than 30,000 of these members work in the public sector as security officers, sworn law enforcement officers, and support personnel. SEIU's law enforcement membership includes the 9,500 police officers in the International Brotherhood of Police Officers.

In support of our work in this sector I have been responsible for developing improved policies and standards for private security, and for coordinating our research and policy work in the federal sector, including in DOE nuclear facilities and NRC-regulated commercial nuclear power plants.

As America's largest security officers' union, SEIU has initiated the only nationwide effort to date to raise standards in the private security industry. We understand deeply the urgency of this task. On 9/11 security officers, janitors, and other building service personnel who are members of our Local 32BJ worked side-by-side at the World Trade Center in New York. Working with the NYPD, FDNY and other emergency workers, they were among the "first responders" to that terrible tragedy, a cause to which many of our members gave their lives. But well before the horrible events of 9/11 SEIU had begun raising the issue of security standards, most notably for airport security screeners.

State laws vary greatly with respect to private security standards and enforcement. Thirty-one states require no training for officers whatsoever. In twenty-one states, private security workers do not have to be licensed. Criminal background checks are not required in sixteen states.

SEIU has also worked closely with governors and state legislators – most prominently in Illinois, California, and New York - to pass legislation to toughen training standards and create greater accountability in the private security industry. We are currently working to pass similar legislation here in the District of Columbia.

Starting in America's larger cities, SEIU has been working with responsible security companies and their clients in the commercial real estate industry, city officials, and public safety experts in an effort to create partnerships between labor, management and government that can address the industry's twin problems of poor training and high staff turnover. Where SEIU, the industry, and its clients are already working together, real improvements are being made that are stabilizing and professionalizing the workforce.

Nearly every major US private security firm including industry leaders Securitas, Guardsmark, and Cognisa are responding to the call for improved private security standards and are working cooperatively with SEIU to improve standards in key US cities.

For example, in June 2004, SEIU - along with the New York Police Department, Mayor Michael Bloomberg, and the Real Estate Board of New York - launched "New York Safe & Secure," a program to provide comprehensive training to security officers in Manhattan commercial office buildings. The program's curriculum was developed with the NYPD, FDNY, and John Jay College.

We welcome the GAO report and share concern over its evidence of problems at five Energy, Science and Environment sites in complying with the Department's new Design Basis Threat. We are especially impressed that the GAO investigators sought security officers' views as their principal data source. Their testimony provides a frank portrait of security at these facilities.

1. CONTRACTORS' FAILURE TO MEET TRAINING AND PERFORMANCE STANDARDS

We know DOE's regulations for training and performance are – as they should be – far beyond the standards in the commercial office world where many of our members are located. But we have had extensive experience with private contractors, both in the security and cleaning worlds and we are acutely aware of the ways in which contracts may encourage or discourage responsible practices. We know that the best standards in the world are weakened if clients – in this case the Department of Energy – do not provide sufficient oversight of their contractors. The GAO report, read in conjunction with other recent reports from the Department's Inspector General's office, give ample cause for concern about the Department's exercise of its oversight role to ensure contractors adhere to the regulations.

The GAO report deals with a number of large-scale matters such as the physical redesign of DOE/ESE sites; the development of new technologies to enhance site security; consolidation of special nuclear material. However we are struck by what at first glance might be construed as the more "prosaic" findings: that officers believe they receive inadequate firearms and tactical training; undependable radio communications (including inadequate batteries); undependable vehicles, some with door handles that do not work which make entering and exiting difficult.

2. WHAT ARE THE IMPLICATIONS OF FAILURE?

Though seemingly mundane, poor communication equipment may in fact contribute to serious problems. We note here the media reports describing problems during a drill at NNSA's Y-12 plant in September, 2004. *The New York Times* reported that guards carrying loaded submachine guns were dispatched to intercept a group of men whom they believed were intruders, but who turned out to be a second team of guards conducting a mock attack with laser-tag equipment. An official from the contractor, the foreign-owned Wackenhut Corporation, said that "communications that night could have been 'crisper.'" Two guards who spoke to the Times, "heard the dispatcher say 'armed suspects' over the radio link, but according to Wackenhut and Energy Department managers, the dispatcher said, 'I have people in the area.'"[1]

Even the most conscientious and hard-working officers cannot overcome problems with training and equipment, which contribute to poor overall security performance and to low morale. There will be very little room for error when the terrorists come, and failure means putting at risk some of the most dangerous material in the world.

If DOE's security budget is nearly $1.5 billion, to what extent is it compromised by poor radios and dead batteries?[2] The solution for problems at this scale is connected to issues we wish to stress, but which are not addressed in the GAO's report: oversight and accountability of contractors' behavior.

3. POOR OVERSIGHT AND ACCOUNTABILITY: INCENTIVES FOR POOR PERFORMANCE

SEIU is not opposed to the use of private security contractors. We believe security should be of the highest standard, whether performed by public authorities or private companies. However, contractors' interest in the bottom line may encourage cheating and cutting corners, unless they are subjected to rigorous oversight. While it is true that these problems exist for public authorities as well, we believe the pressures are considerably greater in the private sphere. In response government must create checks and balances to change the structure of incentives that encourage cheating and cutting corners. We believe, however, that the Department's use of award fees contributes to rather than checks these irresponsible outcomes.

The GAO has consistently warned DOE about problems with respect to award fees, and these problems continue to plague the department.[3] There were a number of high-profile security lapses at the Oak Ridge Complex in the last two years. The most significant was revealed in the Inspector General's report on cheating during security drills.

DOE Investigators found credible evidence that the contractor had committed or tolerated a range of abuses.[4] These included:

- Management told security officers in advance the building and target to be attacked, the exact number of adversaries, and the location where a diversion would occur. This information was reportedly provided about three weeks before the exercise occurred, which allowed the protective force to formulate special plans on how to counter the adversary.
- A protective force responder would be assigned to "tail" the aggressors and observe their movements while they were touring Y-12 buildings and targets prior to and in preparation for an exercise.
- Based on specific attack information, trucks or other obstacles would be staged at advantageous points to be used as barricades and concealment by protective force responders for shooting during the exercises.
- Training prior to a performance test would focus on the specific building to be targeted, and in some instances, an oral plan would be created that deviated from the established Y-12 tactical plan to counter the attack.
- Protective force members had tampered with the Multiple Integrated Laser Engagement System (MILES) gear used to determine whether the officer wearing it could no longer participate in the exercise after receiving a simulated fatal gunshot. Participants had removed the batteries from the MILES gear; put the batteries in backwards and/or placed material such as tape, mud, or Vaseline over the system sensors, so they would not operate properly. New MILES gear purchased at Oak Ridge in 2000, which could have minimized such tampering, was not fully implemented.
- Management would identify the best prepared protective force personnel and then substitute them for lesser prepared personnel who were scheduled to participate in an exercise.
- Officers who would normally relieve other protective force personnel would be armed and held in "stand-by" to participate in an exercise, potentially adding six or seven additional armed responders that would not normally have been available during a shift.

Yet, while the incident cost the contractor about $200,000 in fees, the company still received a "good" performance grade from DOE, an overall score of 93 out of 100 and a $2.3 million fee for the six-month period during which the cheating incident occurred.[5]

The GAO report strongly endorses the importance of force-on-force tests, but their value is eliminated if contractors are able to cheat and provide inadequate training. Rather than a multi-million dollar award, one might have thought that such outrageous practices demanded serious sanctions from DOE, including cancellation of the contract, suspension or debarment. Without serious penalties, the public has every right to ask whether the Department is applying the practice of "social promotion" to oversight of its nuclear facilities.

The range of these practices at Y-12 raises an obvious question as to whether the same contractor behaves similarly elsewhere. Security officers have told us that at least some of these practices are not confined to Y-12. We have heard from multiple security

employees (current and former) at another DOE/ESE, for example, that workers have a common motto when referring to force-on-force tests: "If you ain't cheating, you ain't competing."

Training Cutbacks

The GAO report calls into question the realism of training, a serious problem that was extensively reviewed by the Inspector General last year. The IG reported that various DOE sites "had eliminated or modified significant portions of the training while others were not using realistic training delivery methods." According to the IG, sites that use unrealistic training methods did not meet departmental requirements because the skills acquired by the officers cannot be adequately measured. Moreover, use of anything less than realistic training techniques, "may rob the trainee of the exposure to the levels of force, panic, and confusion that are usually present during an actual attack." Such deviations increase the possibility that the protective force "will not be able to safely respond to security incidents or will use excessive levels of force."

The sites included all of the facilities reviewed in the current GAO report.[6]

But the Inspector General indicated that concerns for security officers' health and safety was not the only factor motivating the contractors' training cutbacks. In some of these cases, Department and contractor security officials indicated that site management was concerned because there was a correlation between the number of injuries incurred at a site and the contractor's performance evaluation rating and subsequent fee determination.

According to an assessment conducted by SEIU, the contractor at the Savannah River site and the Oak Ridge complex had a poor health and safety record at these facilities in 2004, and one might reasonably expect that they had an extra incentive to keep these incidents down.

It is unclear how much the Inspector General's training review has changed practices on the ground, the incentives that encourage such contractor behavior, or how much discipline the department has been able to exert over contractors' short cuts. Last month the Inspector General reported that the security contractor at the Oak Ridge Reservation shorted the protective force on combat readiness refresher training by about 40% on average, reporting "planned" rather than actual training time. The report found that some officers signed attendance rosters for on-the-job refresher training without receiving the training.[7]
The IG also found that Wackenhut officers routinely worked in excess of the 60 hr/week maximum in direct violation of the DOE Protective Force Program Manual. Excessive overtime is itself a form of cost cutting at the expense of security.

We wonder – and believe the Inspector General should investigate - whether these practices are confined to Oak Ridge or are company-wide policies.

Contempt for Oversight Agencies and Congress

This Committee's work depends heavily on the investigations provided by independent agencies, including the Department's Inspector General. Yet for its efforts, the Office of the Inspector General has been subject to continuous public criticism by contractors.

In response to the recent Inspector General report on training problems at the Oak Ridge complex, Jean Burleson, spokesman for foreign-owned Wackenhut mocked the Inspector General as "'bean counters' who didn't understand security practices."[8] In an earlier response to the same report, Burleson was claimed that each of the Inspector General's report on Oak Ridge security in the past couple of years was "fraught with problems."[9]

This manager has a history of public criticism for the IG. In response to last year's report on cheating during security drills, he described details in the inspector general's report as "old news," which he said "may or may not have occurred." He claimed "There is no impropriety right now going on. Security is better today than it has ever been."[10] And in response to the IG's report on training cutbacks across the DOE complex, he said, "Yeah, we had some issues. But make no mistake about it. If you attack us, we are still capable of kicking your a—."[11]

It should be noted that many of these comments came after a this same spokesperson was called to testify before a closed-door Energy & Commerce Committee hearing in January 2004.[12]

Such comments indicate to us a deep-seated contempt for the agencies – including Congress – charged with oversight of these sensitive facilities. These unfortunate comments create an impression completely at odds with oversight and accountability: that companies operate with impunity, and believe they can get away with anything if they have no fear about publicly mocking and denigrating the Inspector General. Moreover, their self-interested claims that facilities are safe may create complacency among the public, or – worse – feed a perception that oversight isn't taken seriously by the Department.

4. FOLLOWING THE CONTRACTORS

To us the conditions described by the GAO report are shocking, but not surprising, since we have encountered very similar problems in other contexts, including NNSA sites, the commercial nuclear power industry and even in sensitive sites such as U.S. military bases. However, the subject matter of the report – and today's hearing – follows the organizational lines of the Department of Energy. This committee has also conducted investigations of, respectively, NNSA sites and commercial nuclear power plants.

While these separate focuses are valuable, they also point to the pressing need for examining security horizontally across such sensitive facilities. From our experience there is a species of problems which is not a product of the specific circumstances of

these different DOE settings, but is instead bound up with the practices of private security companies themselves and the incentives built into their contracts. We have highlighted the incentives for bad behavior arising from inadequate oversight and accountability. While there is certainly value in assessing security within DOE/ESE alone, this choice highlights the additional need to focus on security in a wholistic manner – to follow the contractors across the range of sensitive sites.

Such an approach would be particularly appropriate during procurement, to compel the Department to assess a security contractor's entire record, both in the public and private sectors. While such an approach is required in the Federal Acquisition Regulations, we are concerned that it is not standard procedure in the Department, based on our tracking of last year's award of the INEEL security contract. In February, 2004 Alutiiq – an Alaska Native Corporation with no prior nuclear security experience – was awarded an estimated $200 million sole-source contract for security at INEEL, and was expected to subcontract work to Wackenhut. In this instance, oversight was thankfully provided by the Idaho congressional delegation, which publicly criticized DOE and met with the Secretary of Energy to discuss security at the Lab. In April 2004, DOE quietly announced that INEEL security would not be outsourced after all, effectively reversing the award.[13]

Tracking a company's performance across its scope of operations could uncover patterns that may give cause for concern. An assessment of the security contractor at the Savannah River site, for example, would uncover that the same contractor has been caught cheating by the IG on a security drill; had a poor health and safety record across DOE sites in 2004; cutback on training; performed poorly on a a force-on-force test at the Nevada Test Site; was involved in a near-friendly fire incident; systematically violated weapons inventory and handling policies; shorted employees on training at one facility by 40% on average, reporting "planned" rather than actual training time to the DOE; required employees to work excessive overtime. By widening the scope further to include nuclear power facilities, one would find that the same contractor has been caught retaliating against whistleblowers in commercial nuclear power plants.

The point is that it is the contractor that has boots on the ground; it is the contractor that stands between the Category 1 special nuclear material and the terrorists. Therefore the contractor's record should be under scrutiny.

5. RECOMMENDATIONS

We believe security should be of the highest quality, whether performed by public authorities or private contractors. When using private security contractors, it is necessary to ensure that proper checks and balances are in place to protect against cheating and cutting corners. The DOE nuclear facilities that have substantial quantities of Category I special nuclear material – in both NNSA and ESE – should be the gold standard for the entire security industry.

Such monitoring should begin during the contracting process to ensure that bidders' complete records – both in their private sector and public work – will be subject to scrutiny.

We recommend:

- **That DOE urgently implements an effective process to monitor performance and weed out poor performers, rather than reward them.**

- **That DOE acquisition processes be strengthened to ensure contracting officers do proper due diligence by assessing security contractors' past performance and record of business integrity and ethics.**

- **A review of award fees, and urge the more robust use of penalties as a stick to enforce compliance. The DOE must have a dramatically lower tolerance for cheating and cutting corners, and must make it too expensive for a contractor to risk such behavior.**

NOTES

[1] "Security Drill at Weapons Plant Raises Safety Questions," *The New York Times*, December 21, 2004. The two security guards told *The Times* that they had been threatened with firing if they spoke with outsiders about the incident.
[2] Problems with radios are not limited to the contractor's performance at Y-12; SEIU will soon be releasing a report on security at US Army installations, and guards report that the same contractor is responsible for inadequate provision of radios and batteries at multiple Army bases.
[3] Nearly ten years ago the GAO warned that DOE "contract managers seemed reluctant to use the penalties and sometimes used the financial rewards inappropriately. In some cases, DOE rewarded contractors with award fees, or bonuses, even though their performance was poor." "Department of Energy: Opportunity to Improve Management of Major System Acquisitions," General Accounting Office, November, 1996 (GAO/RCED-97-17), p. 39. In 1999 the GAO reported that DOE could not show how the higher fees it was paying to contractors under performance-based contracting were of value to the government and to the taxpayers. "National Laboratories: DOE Needs to Assess the Impact of Using Performance-Based Contracts," May, 1999, GAO/RCED-99-141, p. 8. As recently as last April, the GAO reported to the Government Reform Committee that many of the problems concerning award fees persist. It recommended that "to ensure the department gets what it pays for," DOE must review how it administers contracts and correct previously identified weaknesses, such as overreliance on contractor data and providing training to its contracting officers." "Department of Energy: Further Actions Are Needed to Strengthen Contract Management for Major Projects," Government Accountability Office, April 19, 2005 (GAO-05-123), p. 39.
[4] United States Department of Energy, Office of Inspector General, Office of Inspections and Special Inquires, "Protective Force Performance Test Improprieties," DOE/IG-0636, January 2004.
[5] "Critics say security still an issue at nuclear weapons plant," *Associated Press*, August 16, 2004.
[6] "The Department's Basic Protective Force Training Program," U.S. Department of Energy, Office of Inspector General, Office of Inspections and Special Inquiries, Inspection Report (DOE/IG-0641) March, 2004.
[7] "Protective Force Training at the Department of Energy's Oak Ridge Reservation," U.S. Department of Energy, Office of Inspector General, Office of Inspections and Special Inquiries, Inspection Report (DOE/IG-0694) June, 2005.
[8] "Y-12 safe, official says: Federal manager at plant disputes recent critical security reports," *Knoxville News-Sentinel*, July 4, 2005.
[9] "Feds assail OR guard overtime; Wackenhut disputes findings by DOE inspector general," *Knoxville News-Sentinel*, June 29, 2005.
[10] "U.S. says guards at nuclear weapons plant cheated in terrorist exercise," *Associated Press*, January 26, 2004.
[11] "Critics say security still an issue at nuclear weapons plant," *Associated Press*, August 12, 2004.
[12] Associated Press, August 12, 2004.
[13] "Craig, Crapo, and Simpson React to DOE Contract Announcement; Abandonment of earlier competitive principles and lack of consultation causes concern," News Release, United States Senator Larry Craig, February 23, 2004. Wackenhut Services, Inc. is a wholly owned subsidiary of the Wackenhut Corporation through which the company administers its sensitive federal contracts. It was estimated that the contract was worth at least $40 million per year for up to five years.

Mr. TURNER. Mr. Walsh.

STATEMENT OF ROBERT J. WALSH

Mr. WALSH. Good morning, Mr. Chairman and members of the subcommittee. On behalf of Under Secretary David Garman, I would like to thank you for the opportunity to appear before you this morning to discuss the readiness of DOE protective forces at facilities which are under the operational oversight of the Energy, Science, and Environment programs.

My name is Robert Walsh. I am currently the Director of Security for Energy, Science, and Environment programs for the Department of Energy. This position was created last year by former Deputy Secretary Kyle McSlarrow, pending the nomination and confirmation of an Under Secretary. The purpose of creating this position was to bring focus and management oversight to security programs on the ESE side of the Department, similar to what the Office of Nuclear Security provides for the National Nuclear Security Administration [NNSA], and to ensure that ESE interests are appropriately represented in the security management decisions of the Department.

Subsequent to his confirmation on June 15th, and his swearing in approximately 1 month ago, on June 23rd, Under Secretary Garman directed that this position be formalized as a permanent part of the staff of the Office of the Under Secretary. The objective and intent of this position is to provide executive management focus for DOE security initiatives as they apply to ESE programs, and to ensure participation and coordination, together with Mr. Podonsky's organization and NNSA, in security decisions and management oversight of DOE security programs.

Although ESE security directors have had two informal meetings since last October, we have taken advantage of the scheduling of this hearing to convene our first official meeting of the ESE Security Management Team since Under Secretary Garman's confirmation last month. In that regard, I am pleased to have with me today security representatives from each of the ESE programs—Environmental Management, Science and Nuclear Energy, Science and Technology—and ESE sites, including Idaho, Savannah River, Oak Ridge National Laboratory, and Richland, which specifically were the subjects of the most recent Government Accountability Office report regarding ESE protective force readiness.

Mr. Chairman, we are here before you today to discuss the readiness of protective forces at DOE's ESE sites. The Government Accountability Office has indicated that they believe that ESE security forces generally do meet readiness requirements as defined by DOE policy directives, and we agree with this assessment.

We are extremely proud of the men and women who comprise the protective forces which are responsible for protecting DOE facilities on a daily basis. These officers are our first line of defense against any active aggression from any number of malevolent sources, and we believe they do an excellent job.

One indication of the overall readiness of protective forces at ESE sites is the fact that special police officer teams from two ESE sites placed first and second at this year's annual Security Protection Officer Training Competition [SPOTC], which was held last

month in Albuquerque, NM and was previously referenced in Dr. Brede's testimony.

Our team from Savannah River finished first among 11 teams, representing ESE and NNSA sites from across the country, with the Hanford Patrol team taking second place in the overall competition. In addition, this year's Police Officer of the Year, Ryan Strader, hails from Savannah River, as does Ryan's colleague, Allen Ford, the second place finisher in the overall individual competition. We are very proud of Ryan and Allen, and the teams from Savannah River and Hanford for their outstanding showing in this year's competition, and I am pleased to recognize them here this morning.

The GAO also identified a number of areas which they felt needed to be addressed, and DOE has either corrected or is working to correct the weaknesses that GAO has identified. I would like to take a moment to briefly summarize our efforts with regard to GAO's specific findings in this report.

First, GAO identified that current DOE policy does not require all protective force officers to participate in every force-on-force exercise, and that sites were not required to formally track individual officer participation in those exercises. GAO recommended that DOE develop policy requirements to ensure officer participation and to require sites to track individual officer involvement.

DOE agrees with these recommendations, and Mr. Podonsky's office has committed to developing and issuing DOE-wide policy to address both issues by the end of this calendar year. We plan to work closely with Mr. Podonsky and his staff to ensure that this is completed.

It should be noted that some ESE sites are already requiring this participation in force-on-force exercises and are keeping track of that participation.

Second, GAO found weaknesses or deficiencies at some ESE sites with regard to equipment issuance or operability, including radio communications, body armor, chemical protective gear, and availability of armored vehicles. We have conducted a comprehensive review of each identified category at each ESE site. We have corrected, or are in the process of correcting each weakness, and we believe that each ESE site is currently in compliance with DOE policy requirements in each case.

Mr. Chairman, we can provide more specific information regarding protective force equipment at your convenience.

GAO has also recommended that ESE develop Department-wide multi-year fully resourced implementation plans to meet the requirements of the new design basis threat. Three of the four ESE sites have participated in the jointly conducted site assistance visits to determine current and future resource requirements of the current DBT. The fourth site, Hanford, is scheduled to be completed in September.

In addition, together with staff from Mr. Podonsky's office, we are currently reviewing the DBT implementation plans from each ESE site. These plans include projected resource requirements and specific timelines, and we believe we are currently meeting all requirements as they have been defined. We expect to complete our

review and submit the plans to the Deputy Secretary for his approval by the end of this week.

Last, GAO recommended that the Under Secretary for ESE establish a security organization to provide management oversight and coordination for security initiatives within ESE programs. As stated earlier, Under Secretary Garman has formalized the position of Director of Security for ESE as a formal part of his management team. We believe that this initiative is responsive to GAO's recommendation in this area.

Once again, Mr. Chairman, I would like to thank you and the committee for the opportunity to appear before you this morning, and I would be happy to answer any questions. Thank you.

[The prepared statement of Mr. Walsh follows:]

Testimony of Robert J. Walsh
Director of Security for Energy, Science and Environment Programs
United States Department of Energy
Before the
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
United States House of Representatives

July 26, 2005

Unclassified Congressional Testimony

Introductory Remarks

Mr. Chairman, honorable members of the Committee, I appreciate this opportunity to appear before you today to testify regarding the current status of Security at Department of Energy sites managed by Energy, Science and Environment (ESE) Programs. In particular, we were asked by the Chairman to focus on the readiness of the protective force, and we are pleased to do so.

As you are aware, the Office of the Under Secretary for Energy, Science and Environment is responsible for the management and operational oversight of Department of Energy programs and facilities that are not otherwise statutorily managed by the National Nuclear Security Administration (NNSA). These programs include the Office of Environmental Management (EM), the Office of Science (SC), the Office of Nuclear Energy, Science and Technology (NE), as well as Fossil Energy (FE), Civilian Radioactive Waste Management (OCRWM), and Energy Efficiency and Renewable Energy (EE). DOE facilities for which ESE programs are responsible include: the Idaho National Laboratory (INL), the Oak Ridge National Laboratory (ORNL), the Savannah River Site (SRS) and Hanford Site, as well as more than 10 additional research

laboratories and operational facilities. The security requirements at ESE sites represent over $400 million of Department of Energy's 2006 budget request

In August 2004, former Deputy Secretary McSlarrow created a temporary position of Director of Security for the Office of the Under Secretary for Energy, Science and Environment in order to provide "expert advice and assistance on security-related issues to the Under Secretary." Mr. McSlarrow directed that this position "serve as a focal point for all ESE security activities and provide a clear interface between ESE and the Office of Security and Safety Performance Assurance (SSA)." I was assigned to that position by the Deputy Secretary at that time.

On July 3 of this year, Under Secretary David Garman formalized the position of Director of Security for ESE Programs within the Office of Under Secretary. The creation and formalization of this position ensures that the Office of the Under Secretary for ESE will now have a focal point for ESE and DOE security issues and that ESE will more effectively participate in Department-wide security management decisions with counterparts in SSA and NNSA. This further ensures that ESE will maintain its share of DOE's security partnership between our organization, DOE's policy organization (SSA) and security operations within NNSA. This partnership is extremely important in order for DOE to ensure sound and balanced management oversight over the Department's security programs. I can assure you that we are very cognizant of the security challenges which we face in a post "9/11" threat environment, and Under Secretary Garman, together with Secretary Bodman and Deputy Secretary Sell are all personally engaged

and fully committed to ensuring that those challenges are met for the entire DOE complex.

Energy, Science and Environment Security (ESE) Program Offices are responsible for the management, operation, and oversight of a variety of DOE sites involving a wide range of activities including energy, biological and environmental science research, environmental cleanup, and nuclear engineering and technology. ESE's responsibilities include management of four principal sites (Hanford, Savannah River, Oak Ridge National Laboratory, and Idaho National Laboratory) which contain some quantities of Category I Special Nuclear Material and which were the focus of a recent review by the Government Accountability Office (GAO). We are here today, in part, to provide information related to the findings contained in that report.

First, it is important to state that the Department of Energy is extremely proud of the men and women who constitute the protective forces which are responsible for protecting DOE facilities and assets on a daily basis. We hear regularly from a variety of government auditors and investigators from a number of organizations such as GAO, Congressional staff offices, the Inspector General's Office and the Office of Independent Oversight that they are all favorably impressed with the overall professionalism and dedication of our protective force officers. These officers are DOE's first line of defense against any act of aggression by any number of malevolent sources and we believe that they do an outstanding job on a regular basis.

At Energy, Science and Environment (ESE) sites, over 1,000 protective force officers routinely provide protection at four major facilities housing Category I Special Nuclear Materials. We believe that the officers assigned to these ESE sites including Hanford, Savannah River, Oak Ridge National Laboratory, and Idaho National Laboratory are among the best trained, best equipped, and most responsive of any across the DOE complex. One indication of the overall readiness of ESE protective forces is the fact that special police officer teams from two ESE sites placed first and second at this year's annual Security Protection Officer Training Competition (SPOTC) held this year from June 5 through 9 at Albuquerque, New Mexico. The team from the Savannah River Site finished in first place among 11 teams representing ESE and NNSA sites from across the country, with the Hanford Patrol team placing second in the overall competition. In addition, this year's Police Officer of the year, Ryan Strader, hails from Savannah River with his Savannah River colleague, Allen Ford placing second in the overall individual competition.

The Office of the Under Secretary for ESE is extremely proud of the significant accomplishments by these outstanding officers.

GAO Report Observations

Please allow me at this point to provide several comments on the recent report provided to you by the Government Accountability Office (GAO) entitled "DOE's Office of Energy, Science and Environment Needs to Take Prompt Action to Meet the New Design

Basis Threat." GAO conducted this review at four ESE sites from late 2004 through early 2005. The focus of this review was to determine whether DOE/ESE protective forces were able to meet current threats as set forth in DOE's most recent Design Basis Threat, whether they were sufficiently trained and equipped and to evaluate their level of confidence as to their ability to perform their assigned duties.

In general, GAO found that DOE/ESE protective forces do currently meet established readiness requirements, that officers are confident in their overall readiness and level of preparedness to execute their duties, that they generally meet all DOE training and equipment requirements, and in most cases, either carry or have access to standard protective force equipment.

However, GAO did note some weaknesses in protective force requirements and practices at ESE sites which I will address briefly at this time:

Force-on-Force Participation

During their review, GAO found that not all protective force members were required to participate in force-on-force exercises on a regular basis. In addition, the report found that DOE policy does not require sites to track protective force member participation in these exercises.

DOE's Office of Security and Safety Performance Assurance, which is responsible for issuing security policy, has advised that it intends to issue new policy which will ensure that protective force officers are required to participate in force-on-force exercises on a regular basis and that such participation will be required to be tracked and documented in appropriate training records at each site. We agree that this should be done.

Weaknesses in Protective Force Equipment

The review found that at some ESE sites there were deficiencies or weaknesses in protective force access to adequate equipment such as dependable radio communications, body armor, and chemical protective gear.

DOE subsequently conducted a review of protective force equipment at each ESE site in each of the areas identified by GAO. We believe we have substantially improved or corrected all deficiencies identified and that all ESE sites are currently in compliance with DOE policy regarding protective force equipment requirements.

Implementation Planning for the 2004 Design Basis Threat Requirements

GAO recommended that DOE/ESE develop Department-wide implementation plans for meeting the requirements of the 2004 Design Basis Threat. DOE sites were directed in October 2004 to prepare implementation plans for submittal in July 2005. ESE implementation plans have been received and are currently in the review process. These plans are scheduled to be provided to the Deputy Secretary by the end of July 2005.

Planning for the Creation of an Elite Force

The GAO report recommended that the necessary policy revisions be undertaken to support the implementation of an Elite Force initiative.

The Office of Security and Safety Performance Assurance has advised that policy revisions regarding this initiative are currently being written and are scheduled to be submitted for final departmental approval no later than the end of December 2005.

Development and Deployment of Enhanced Security Technologies

GAO recommended that DBT implementation plans include planning for the development and deployment of enhanced security technologies.

The Department of Energy security community is committed to exploring and acquiring newer, better, and more cost effective ways to provide state of the art protection for DOE facilities. DOE's Office of Security and Safety Performance Assurance has a number of initiatives in place to ensure that these technologies are adequately reviewed, evaluated and deployed. ESE sites are evaluating use of these technologies as they prepare their Design Basis Threat Implementation Plans.

Transportation and Consolidation of Special Nuclear Material

In February 2005, the Secretary established the Nuclear Materials Disposition and Consolidation Coordinating Committee which is chartered to identify opportunities for material disposition and consolidation across the complex. Led by the Secretary's National Security Advisor, the NMDCCC is charged with considering all aspects of materials consolidation to include impacts on operations, transportation assets, and realistic schedules. Under Secretary Garman is a co-chair of the Executive Steering Group (with Ambassador Brooks from NNSA) for this initiative and ESE organizations are actively participating in the Committee's efforts to consolidate nuclear materials at fewer DOE sites.

Establishment of an ESE Security Organization

One of GAO's recommendations was for the Under Secretary for ESE to establish an organization to oversee development, implementation, and coordination of ESE and broader DOE efforts to meet the 2004 Design Basis Threat. As stated earlier in my testimony, Under Secretary Garman has, in fact, created the position of Director of Security for ESE Programs which will be responsible for the day to day management, coordination, and operational oversight of ESE security programs. This position will work closely with ESE Program Secretarial Officers and their respective security managers and will ensure appropriate interface and coordination with counterparts in the Office of Security and Safety Performance Assurance (SSA) and the National Nuclear Security Administration (NNSA).

This concludes my prepared remarks, Mr. Chairman. At this time, I would be pleased to respond to any questions from the Committee.

Mr. TURNER. Thank you.

We will begin questions for the panel with our chairman, Chairman Christopher Shays. We will begin with a 10 minute round of questions.

Mr. SHAYS. I thank the chairman for giving me this opportunity to ask questions and to say I was in Iraq 24 hours ago, so I am trying to listen, but it is a little difficult.

We have had three hearings with the Under Secretary for the National Nuclear Security Administration, and this is our second hearing on the Under Secretary for Energy, Science, and Environment. There are only two Members here. I don't know that is an indication that people think we are doing well or whether there are just so many things to focus on.

However, I happen to think this is a hugely important hearing, and I thank you all for being here. I am not sure if the chairman and I will direct questions to everyone, so I have no problem with others jumping in if they want to respond to questions.

Mr. Podonsky, you seem to come to either hearings we have, given that you are involved in both areas, is that correct?

Mr. PODONSKY. Yes, sir.

Mr. SHAYS. How would you evaluate ESE's efforts to implement the design basis threat denial of access security strategy?

Mr. PODONSKY. Until Under Secretary Garman was confirmed and until Director Walsh was put into his position, I would characterize ESE as being somewhat slower in what we had anticipated or hoped for implementation of the DBT. Part of that we believe is because the ESE organization was made of very strong, sincere individuals for their security programs within ESE, science, nuclear energy, environmental management, fossil energy.

The reality is they were all doing what they thought was prudent for their particular sites. We did not see the rapidity that we felt that was needed to implement the design basis threat, but they all had their individual perspectives on what their priorities were. I don't want to speak for what their priorities——

Mr. SHAYS. Let me get to the next question.

Mr. PODONSKY. Yes, sir.

Mr. SHAYS. How do you evaluate the ESE? Are you optimistic that they are going to meet their 2008 deadline on the design basis threat?

Mr. PODONSKY. Yes, sir, we are guardedly optimistic that they will because they have the new leadership that they have not had in the history of the ESE before. And that guarded optimism comes from the implementation plans that we have recently read from Idaho and one of the other sites within ESE. We hadn't seen that enthusiasm before.

Mr. SHAYS. What kind of program office resistance have you encountered regarding the implementation of the design basis threat?

Mr. PODONSKY. If I said resistance, I misspoke. I think what we have seen is extremely careful analysis of what the design basis threat was and how it applied to their sites. The other thing that I think, in all respect to the Department, the design basis threat from May 2003 changed in October 2004. So we would expect that ESE sites, like the NNSA sites, should be moving toward completion of the 2003 DBT numbers in 2006 for completion.

Mr. SHAYS. I have a sense that the Department is reluctant to implement the design basis threat. You don't think there is a reluctance?

Mr. PODONSKY. We have seen a hesitancy in terms of the Department——

Mr. SHAYS. That is called a reluctance.

Mr. PODONSKY. Yes, sir.

Mr. SHAYS. OK. So you have seen that.

Mr. PODONSKY. Yes, sir.

Mr. SHAYS. OK. Why did DOE change the design basis implementation deadline from October 2007 to October 2008?

Mr. PODONSKY. I am not familiar with the October 2007 deadline being changed to 2008. There was a review that former Deputy Secretary McSlarrow asked for to be conducted at the end of a series of this committee's hearing and the GAO report on the NNSA facilities.

Mr. SHAYS. I will throw this out to you and then anyone else who wants to answer. The design basis threat, if it isn't met until 2008, we are basically stating that we are vulnerable. That is what it says to me. In other words, we can't meet what we believe is the threat. So I guess what I have a hard time understanding is why does it have to take 3 years? It doesn't seem like it is rocket science to me. It seems to me it is just a matter of doing it.

And I am going to throw this out to anyone else who wants to answer.

Mr. PODONSKY. Mr. Shays, if I could start off, if my colleagues here at the table will permit me. From an NNSA perspective, my organization, that has both policy and oversight of the Department, safeguarding security and cybersecurity, to name a few subjects, we don't disagree with the perception and the reality that if you have a threat today, how can you not meet it until 2008 and beyond.

What we believe has been a great distraction for this body, as well as the executive branch, is the focus on the policy of the design basis threat, when in reality it should be about implementation: the application of new technologies, the elite force that we have mentioned in our testimonies here today, how we apply our security strategies at our sites, and, equally as important, nuclear material consolidation.

It gets confused between both the legislative arm and the executive branch on focusing on the policy and the threat, when in fact we need to have our sites implement a more robust security posture than we currently have if we are going to meet today's challenges that we see throughout the world.

Mr. SHAYS. I don't really feel that you have given me an answer to the question, though. Why does it have to take so long?

Mr. PODONSKY. I don't have an answer why it should take so long.

Mr. SHAYS. OK.

Mr. Walsh.

Mr. WALSH. Mr. Chairman, the only thing I would add is, and I spent some time in intelligence and working on postulated threat and design basis threat. The design basis threat is, and we have to be careful that we don't wind up getting into anything classified, and make sure we don't. But the design basis threat is a generic

threat on which you design your protective forces and your protection strategy over a very long period of time, usually 15 or 20 years. For many years the design basis threat was fairly stable. I think post-September 11th, realistically, we have to take a very close look at that.

Mr. SHAYS. Well, you had to take a close look. For instance, if you believed that people who came in to get one of the resources that we were protecting, if you believed that they didn't want to lose their lives, were willing to risk losing lives, but didn't want to lose their lives, you believed that they also had to get out with the material. So you had a design basis threat that said, well, maybe they can get in, but they are not going to get out.

Mr. WALSH. Right.

Mr. SHAYS. But if you, all of a sudden, realize that they don't care if they get out, if they are willing to blow themselves up onsite, the design basis threat changes, correct?

Mr. WALSH. Parts of it change. The strategy may change.

Mr. SHAYS. Well, wouldn't it mean that you might have accepted their getting in, but now you can't even let them get in? And doesn't that mean, then, that your whole resources have to change and your whole strategy has to change?

Mr. WALSH. Well, they do. But it is more than just the strategy of your adversary; it is the numbers of adversaries and numbers of other things, and their capabilities that go into——

Mr. SHAYS. Right. But if you feel, for instance, that the design basis threat was that they were only going to have one insider who is helping, and you decide that there is going to be two out of the logic that there could be two——

Mr. WALSH. That would change it.

Mr. SHAYS [continuing]. Then your design basis threat has changed, correct?

Mr. WALSH. That would change it.

Mr. SHAYS. My question, though, is given that this is an incredible resource that we are trying to protect, why would we tolerate having to wait 2, 3, 4, or 5 years? That is what I don't understand.

Mr. WALSH. I know I am not understanding your question, but——

Mr. SHAYS. But you aren't answering the question. But why? What is so difficult about a design basis threat that it has to take 4 or 5 years?

I will leave that on the table and go to the chairman. I am going to come back to that.

Mr. WALSH. OK.

Mr. TURNER. Well, to pick up where the chairman has left off, Mr. Podonsky, you made a statement that troubled me. You said that this body has a design basis threat focus. And I was just conferring with counsel here. My recollection is the design basis threat process is not one that Congress has imposed upon you. You have just acknowledged that is the case. So we are left in doing an evaluation of whether or not you are sufficiently protecting these very dangerous assets.

In reviewing your bureaucratic processes—and that is what concerns me most, is that we are talking about a bureaucratic process—you come up with a design basis threat and you determine

whether or not you are going to meet it. You go through a process to assess what it is going to take to meet it.

And I think that sometimes people don't get their heads up from their desks enough to look out of the window and say if you are actually sitting in front of this body and saying you are not going to meet the design basis threat until 2008, and it is a threat that we all acknowledge exists today, not in 2008—Mr. Walsh, I disagree with your statement of a 15 or 20-year time period. You are not projecting what the threat is in 2008; you are projecting what the threat is today, and you are trying to meet it by 2008. Is that correct?

Mr. WALSH. You are making an assessment of the most likely or representative threat that you need to protect against and you need to design your protection strategy against that. Because of the nature of the design basis, it should stay fairly stable over a long period of time.

Mr. TURNER. Does the design basis threat that you are currently trying to meet in 2008 represent a capacity for a threat at these facilities today? That is a pretty easy question.

Mr. WALSH. Well, not really.

Mr. TURNER. I mean, either you believe that what is currently in your design basis threat that you are projecting to meet in 2008 is not a threat that is lurking out there today or you think it is. And if you think it is, and you are saying that you are going to meet it by 2008, then what you are saying is that DOE is not currently meeting the threat that is out there today.

Mr. WALSH. Well, first let me say that we on the ESE side, as well as NNSA, are committed to meeting the design basis threat, as it is presently laid out for us in the 2004 policy that we have; and that is what we are moving toward meeting. Now, the question of validity, what I can tell you is——

Mr. TURNER. Well, perhaps let me ask it again. Are you telling me, then, that you do not believe that the design basis threat that you are attempting to meet by 2008 represents the threat that exists at these facilities today?

Mr. WALSH. The most likely or most representative threat?

Mr. TURNER. Does it meet a threat that you are facing today? It is either yes or no.

Mr. WALSH. No, I am sorry, Mr. Turner.

Mr. TURNER. If you don't believe it is out there, then that is a whole other issue for us to pursue. Do you believe that the design basis threat, that you are trying to meet by 2008, represents a threat that exists to these facilities today?

Mr. WALSH. Mr. Chairman, I am sorry, it is more than a yes or no answer. It has a lot to do with the numbers and the capabilities and the strategies that you address with the numbers of people that you assume are going to come at you. It is not really a yes or no answer. And it is based on intelligence assessments and postulated threats. So I apologize, but it is more than a yes or no answer.

Mr. TURNER. Well, I disagree. And I am very disappointed in the position that you have for security in DOE, that you would say that you can't answer yes or no. So we will just go down the panel.

Mr. Aloise, do you believe that the design basis threat that they are attempting to meet by 2008 represents a threat that exists to these facilities today?

Mr. ALOISE. In our view, that is DOE's criteria, and that is what we measure them against.

Mr. TURNER. Mr. Friedman.

Mr. FRIEDMAN. That is my understanding of the criteria for the construction and development of the design basis threat essentially, yes.

Mr. TURNER. Mr. Podonsky.

Mr. PODONSKY. It was written by my office, so my answer is yes.

Mr. TURNER. Dr. Brede.

Dr. BREDE. That is a policy question from an implementation standpoint. We are preparing to deal with that threat today.

Mr. TURNER. That is not an answer.

Dr. BREDE. We posit that threat exists today. That is my opinion.

Mr. TURNER. Thank you.

Dr. Adler.

Dr. ADLER. I will pass and say the last time I looked the DBT was classified information, and I lack a security clearance, so I am not capable of answering it.

Mr. TURNER. It is just an opinion as to whether or not you think that the threat is out there today.

Dr. ADLER. Again, the specifics of what the DBT consists of are not something that is shared with ordinary citizenry. What I would say is what is put out in the news about what this could consist of isn't something that will happen in the future, it has already happened. We have already been attacked by such force.

Mr. TURNER. Mr. Walsh.

Mr. WALSH. Yes, sir.

Mr. TURNER. Do you want to change or supplement your answer, or is your answer still so complex that I can't decide if it is yes or no?

Mr. WALSH. Well, two of the previous answers said that it is the criteria that they measure to.

Mr. TURNER. That is why I found your answer confusing, because my understanding of what the design basis threat was based on today's threat, not a projection of the threat in 2008. And your answer was that it was the threat 10, 15 years out in the future.

Mr. WALSH. It is a generic threat by which you design your protective forces and your protective strategies that you hope will be static for a number of years, 15 or 20 years. Now, you have to adjust that, and we have a review process for that every year. But the design basis threat is your most likely or most representative threat over a long period of time. I agree with two of the——

Mr. TURNER. So does it represent a threat that these facilities have today? Does that long period of time that you are describing to us include today?

Mr. WALSH. If you are asking if the design basis threat is the most representative or most likely threat against DOE facilities today, I would have to say I am not sure. We are going through a review right now.

Mr. TURNER. Mr. Chairman.

Mr. SHAYS. Mr. Walsh, you are trying to answer honestly, but I feel like you are Mr. Ford, telling us well before Eastern Europe was free, that it is free. And I would like you to kind of catch your breath a second.

Mr. WALSH. OK.

Mr. SHAYS. It is not a difficult question to answer. The design basis threat is the threat we believe exists today and will exist in the future. We constantly are changing the design basis threat. The fact that we can't be ready until 2008 means that we are not ready. And that gets to a question that I am going to pursue again.

But, frankly, your answer is alarming. Or it just shows that you don't believe in the design basis threat. In other words, obviously, in the end, it is an opinion. It is an opinion, with a lot of different people, that this is the threat that we have to protect against. If you, in your mind, think that it doesn't represent an accurate threat, that is an answer that you can say, and you disagree with the design basis threat. So let us go there.

Do you agree with the design basis threat or do you disagree with the design basis threat, that is, we are not going to talk about what it is, but do you agree with it?

Mr. WALSH. Once again, let me state for the record that we are committed to the design basis threat as it is stated and we are moving toward preparing for that through 2008.

Mr. SHAYS. I hear you.

Mr. WALSH. Because that is the Department policy. The Deputy Secretary has asked us to review that right now, and we are undergoing an internal review of the DBT. But to restate it, if you are asking me if I think the design basis threat right now, as it is stated, is the most likely or most representative threat against a DOE facility——

Mr. SHAYS. I didn't really ask it that way, because the design basis threat isn't necessarily the most likely.

Mr. WALSH. It is the most representative.

Mr. SHAYS. No. The most likely, it also has to be what we believe we ultimately have to protect against.

Mr. WALSH. Right.

Mr. SHAYS. It may mean that the design basis threat includes what we think is not as likely as something else, but we at least have to get up to that level. We may think it is more likely that—and since I haven't looked at the design basis threat, the numbers I am throwing out right now these numbers are made up.

But, for instance, if we thought the design basis threat involved the fact that you could have two people on the inside working with people on the outside, but we think it is more likely it will be one, but we still have to prepare for two, yes, it is more likely that it may be one, but we still believe that we have to have our design basis threat to deal with two because it is still a possibility that we know we have to protect against.

So when you say what is most likely, that is not really what I am asking. I am asking you a question: are you working in this administration and are you on that side of the equation that disagrees with the design basis threat, and is that shaping your response? Because that is the only way I can justify your answer.

Mr. WALSH. Well, the only thing I can say, sir, is that I think that it is worth it to make sure that whatever the design basis threat is, that it is right, that we get it right.

Mr. SHAYS. OK.

Mr. WALSH. And we are in the process of reviewing it now. It might very well——

Mr. SHAYS. And the question I have is do you disagree with the present design basis threat? That is not top secret, you can say yes or no. I haven't asked you what it is.

Mr. WALSH. No, I understand that.

Mr. SHAYS. OK. So are you on that side of the equation that disagrees with it?

Mr. WALSH. I am not totally convinced that the current intelligence foundation that really does go into developing a design basis threat supports where we are right now.

Mr. SHAYS. That is a fair question. Now, if that is shaping your response to the first question——

Mr. WALSH. I believe it is.

Mr. SHAYS. OK, but it shouldn't, because the real question is, in terms of policy, the design basis threat—the answer to the question is the design basis threat is what we believe, based on what we have agreed to, is a threat that we have to protect ourselves against; not necessarily the most likely, it is a threat we have to be able to protect ourselves against, and we test ourselves against that.

Mr. WALSH. Right.

Mr. SHAYS. Then the answer to the question is a single yes, it exists today. That is the simple answer to the question. The design basis threat is the threat we believe exists today. Is that not true?

Mr. WALSH. That is true.

Mr. SHAYS. Yes. And that is the better answer.

Mr. WALSH. That is true.

Mr. SHAYS. So we are going to sort out all your past answers and that is an——

Mr. WALSH. OK. Thank you, sir.

Mr. SHAYS. And we are not badgering you into giving us that answer; that is the answer.

Mr. WALSH. I appreciate that.

Mr. SHAYS. OK. And I appreciate your disagreement with the design basis threat, and that is fair. You have a right to disagree. And you have a responsibility to tell us if you disagree. So that is an honest dialog.

But what I am having trouble with is given that we think the design basis threat is the threat we believe exists today, waiting until 2008 or 2007 to protect ourselves against it is a little unsettling.

My question, and I will go with GAO and our Inspector General to start us off in this—it seems to me that obviously, if you change the design basis threat and you say that it is two insiders instead of one, all of a sudden everything changes. Isn't that correct? I mean, if you are protected against one, and now you have changed it so you have two insiders, then you have a different task? Can both of you agree?

Mr. ALOISE. Yes.

Mr. SHAYS. Mr. Friedman.

Mr. FRIEDMAN. Yes, I agree, Mr. Chairman.

Mr. SHAYS. OK. Or you may decide that if you said it was going to be 15 people, and now we think potentially 20 people might attempt in some way to come in, that may change the design basis threat. Is that correct?

Mr. ALOISE. Yes.

Mr. SHAYS. A nodding of the head doesn't get recorded. Mr. Friedman.

Mr. FRIEDMAN. Yes.

Mr. SHAYS. Thank you. If you believe that someone might use aircraft in a way that we didn't anticipate, but now we say they may use aircraft, that changes the design basis threat as well, is that correct?

Mr. ALOISE. That is correct.

Mr. FRIEDMAN. I think it does, yes.

Mr. SHAYS. OK, both responded in the affirmative.

Now, given whatever caused us to change it, tell me what I need to know beyond this: you may need more people or you may need those people trained differently; you may need some technical capabilities that you didn't have in the past; or you may have to do structural things just with the site.

In other words, candidly, when we were looking at Mr. Brooks' operation and one of the sites there, we thought a lot of old buildings, not a lot of clear sight lines. You need to get rid of some of these buildings; there are a lot of places to hide.

So is there anything other than structural, technical, or people that go into responding to a design basis threat? And I am not saying that there isn't; what other ones out there? I am just trying to understand why it is difficult, why you have to take 3 years. That is what I am trying to understand. So you want to give me a——

Mr. ALOISE. That about sums up a lot of what you would need to do.

Mr. SHAYS. Is your mic on, sir?

Mr. ALOISE. Excuse me?

Mr. SHAYS. Is your mic on?

Mr. ALOISE. Yes. One thing would be also the consolidation of materials in fewer places would increase security, and you could develop your design basis threat around that as well.

Mr. SHAYS. And that could take time to consolidate.

Mr. ALOISE. Sure. Yes.

Mr. SHAYS. But it is also true that in the short-run you might over-utilize people to compensate for the fact that in the future you can consolidate and even use less people than you are using presently. In other words——

Mr. ALOISE. You would use less people, of course, at the places where you took the material from.

Mr. SHAYS. When you consolidate, that enables you to focus your attention; collectively you are using less people. But in the short-run, until you consolidate you may have to use more people.

Mr. ALOISE. Right.

Mr. SHAYS. Even more than exists right now. In other words, you look at it and say we have this number of people and they are trained, but the challenge is we think that we are vulnerable with

this new design basis threat. We can do it two ways: one is we can add more people or we can take these three sites, make them one site, or two sites and make them one, and even use less people. But one takes longer, so you might have a short-run solution until you get to the long-run solution. Which gets me to this basic point: Why does it have to take 3 years to protect ourselves?

I will throw that open to anyone.

Mr. FRIEDMAN. Mr. Shays, can I? I come here as an IG, of course, wearing several hats, but one of which is ensuring that we spend our money prudently and in the right way. While I agree the ideal is once you have an agreed upon, approved design basis threat that is based on sound intelligence and all the rest, the ideal is to have virtually an instantaneous defense for the threat that has been postulated in the design basis threat. That is, where we should be looking for. And I am not sure that the time that we have currently have in mind is an acceptable level, and I agree with your point on that.

But we want to make sure, as well, that we spend the money wisely and get the money. We have to get the money, we have to spend it wisely, and make sure it is spent in the right locations and it is prioritized properly. And there are some time constraints that are involved there.

I was going to mention the consolidation of material as well. That is not an overnight process, and you have analyzed that quite properly, I think.

So while I am not here defending the Department, I am here trying to make sure, as well, that we spend the money appropriately, we award contracts properly and do all the things that have to be done in Government——

Mr. SHAYS. Mr. Friedman, let me just be very clear. As Inspector General, I don't ever view that your job is always to criticize the Department. Sometimes you criticize it and sometimes you defend it. And you should never be embarrassed by defending the Department, helping us understand.

Mr. Podonsky.

Mr. PODONSKY. Mr. Shays, if I could offer an alternate view, and it goes back to my earlier statement that Mr. Turner responded to. If I might go there first, because of my bringing in the legislative arm and the executive branch. I was not criticizing either body; I was making an observation that we are focused on a policy that is important, but I too don't have the responsibility for programmatic implementation.

So it is easy for me to criticize, as an independent overseer, and my criticism from my organization is the following: It shouldn't take enormous sums of money to meet the threat that we think we are dealing with if we start out with changing our protective strategies, if we start applying new technologies that are actually some off-the-shelf, if we begin changing the way we train our elite force that we already have in place—not our elite force, but we already have our special operation forces that are trained to be responsive to different events. We need to start training them differently, similar to the way my oversight trains its composite adversary team.

The nuclear material consolidation piece is in fact probably the more daunting challenge because of State requirements and regulations, and where we are going to put all the material. But I would offer to you we also, in SSA, share the same concern about the length of time that it takes to implement the new DBT, which is connected to budgetary cycles because people think that they need an enormous amount of more money.

My colleague in the Inspector General's office thinks it is going to take an enormous amount of money; our colleague at GAO thinks it is going to take a lot more money. And I would offer to you that, yes, there will be more money, but not the amount of money that everybody is talking about if we use the resources we have at our sites today and use them in the 21st century.

Mr. SHAYS. My time has run out for this line, but let me just say the feeling that I get when I think that a design basis threat can take 3 to 4 years to get up to, it really says to me that it is almost the attitude that Mr. Walsh has, that, you know, the design basis threat almost represents the extreme and not the unlikely; and, therefore, we don't mind if it takes 3 years. That speaks volumes to me about the attitude. It is really a statement that says that we can do that and take that lump.

Mr. TURNER. I recognize Mr. Dent from Pennsylvania.

Mr. DENT. Thank you, Mr. Chairman.

Mr. Podonsky, my question is directed to you. GAO believes that the ESE will not be able to field an elite force by the October 2008 DBT implementation deadline. You disagree. Why is that?

Mr. PODONSKY. I disagree that the Department will not be able to have the elite force requirements and policies in place as scheduled. The elite force concept was a concept that was born last year under previous Secretary Abraham's security initiatives, and the concept originally started out as whether we should Federalize the forces or have them as contract guards.

And through an evolution of discussions with both ESE and NNSA and field implementers, it was determined that what is really needed at our sites is the capability to respond differently to the different events at our sites. Specifically, whether it be NNSA sites or ESE sites, the traditional response by this Department has been more of a law enforcement "respond to the bank robbery" response as opposed to more of a military tactical response. We are moving toward that tactical implementation now.

For the last year, since the anouncement of the initiative of the elite force became a reality in terms of the initiative taking hold, there have been multiple meetings and policy implementation changes, and by the end of the year the part that I own and am responsible for the Department, in terms of issuing policy, putting out new standards, that will be done. Now, whether or not ESE and NNSA step up to the requirement, I can't speak for the implementers; that would be better answered by Mr. Walsh or by Mr. Desmond from NNSA.

Mr. DENT. Thank you, Mr. Podonsky.

Mr. Aloise, I have a question for you. How would you evaluate ESE efforts to implement the DBT denial of access security strategy, and do you think we can make the 2008 deadline for the DBT implementation?

Mr. ALOISE. Not by business as usual. We are calling for a comprehensive plan that outlines how they are going to develop the elite force, how they are going to consolidate materials, how and where they are going to develop and deploy technologies. We believe that this is a big endeavor, and you need a very smart plan to show Congress and others how you are going to get there.

Mr. DENT. Thank you.

No further questions.

Mr. TURNER. Mr. Kucinich.

Mr. KUCINICH. I thank the Chair. Sorry I wasn't in earlier; there was a trade bill on the floor I was in debate on. So I appreciate the chance to ask some questions.

I would like to begin with Mr. Podonsky. There have been hundreds of news stories over the last year related to security incidents at the Department of Energy facilities guarded by Wackenhut, specifically the Nevada test site and Y–12. There have been at least four Inspector General investigations in the past year relating to Wackenhut's performance.

And I understand the Nevada test site security contract, currently held by Wackenhut, is out to bid right now. I also understand from recent news reports that the two security contracts held by Wackenhut in Oak Ridge are to be put out to bid together this summer.

In the face of questions over Wackenhut's performance, what is the tolerance at DOE for a security contractor that creates an image problem, if not a security risk?

Mr. PODONSKY. I think that question would be more appropriate for Mr. Walsh, but let me start out with giving you the perspective from the SSA. We oversee the Department in terms of its performance, and the performance tests that we have run over the many years have demonstrated a mixed review on the capabilities of the Wackenhut guard force. But when we have done these inspections, like at Nevada test site, the corrective actions we have seen taken by both the Federal and the contractor, have been appropriate to resolve our concerns, and then we go back and retest them.

Mr. KUCINICH. So you are telling this subcommittee you really don't have any concerns about Wackenhut right now?

Mr. PODONSKY. We don't look at Wackenhut as a corporation for concerns. We look at the performance at each site.

Mr. KUCINICH. About their performance. Well, of course. That is what I am talking about.

Mr. PODONSKY. But as a corporation or as a contractor, that would be better answered by Mr. Walsh.

Mr. KUCINICH. OK, Mr. Walsh. Thank you, Mr. Podonsky.

Mr. Walsh.

Mr. WALSH. I am sorry, Mr. Kucinich, I wouldn't have any information on that. We work on the ESE side, and you mentioned the Nevada test site, which I don't really have any knowledge of. I can only say that the few times that I have been involved with direct oversight of Wackenhut contracts, for instance, at headquarters, I felt that they performed in more than an adequate way. So that would be the only information I have.

Mr. KUCINICH. Well, let me ask you this, either you or Mr. Podonsky, if you could answer this question. You had the recent IG report on training and overtime problems at Oak Ridge.

Mr. WALSH. Right.

Mr. KUCINICH. And it recommended that the managers of Oak Ridge and Y–12 site officers, "evaluate the impact of the issues discussed in this report on Wackenhut's award fee." Can you or Mr. Podonsky inform this subcommittee of the progress of this recommendation since the report was issued?

Mr. PODONSKY. I can tell you relative to answer your question. Our inspection team went down to Y–12 recently, in the last couple months, and we saw a vast improvement over the last three inspections of the performance at Y–12. Specific to the recommendation, I couldn't give you a current status, but I can tell you that the performance of the protective force that we saw at Y–12 far exceeded the last 6 years of our inspections.

Mr. KUCINICH. You say you can't give us an evaluation in current performance?

Mr. PODONSKY. No, I gave you the evaluation of the performance of the protective force in performing their duties through the force-on-force test that we conducted and the training that we reviewed. But relative to award fee and any other recommendations, I couldn't tell you where the program office is on that.

Mr. KUCINICH. Is there any way you can get that information and get it to the committee? Is anyone here responsible for that who could get that information to this committee?

Mr. WALSH. We can take it for the record, sir, absolutely.

Mr. KUCINICH. Can you do that?

Mr. WALSH. Yes, sir.

[The information referred to follows:]

COMMITTEE:	HOUSE GOVERNMENT REFORM, SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS
DATE:	JULY 26, 2005
WITNESSES:	ROBERT J. WALSH AND GLENN S. PODONSKY PAGE 65, LINE 1485

INSERT FOR THE RECORD

The Inspector General issued a report entitled "Protective Force Training at the Department of Energy's Oak Ridge Reservation" on June 24, 2005. One of the recommendations contained in that report stated that the Manager, Oak Ridge Office and the Manager, Y-12 Site should "Evaluate the impact of the issues discussed in this report on Wackenhut's award fee" for their respective contracts with Wackenhut Services, Inc.

The Security Director at the Oak Ridge Field Office advised that because the contract period ended on June 30, 2005, there was not sufficient time to consider the IG recommendations for that award fee period, but that the impact of the issues discussed in the report will be considered at the end of the current period which ends on December 31, 2005.

Mr. KUCINICH. Mr. Chairman, I just want that acknowledged.

And, finally, Mr. Podonsky, many of the Department's security upgrades could be limited by consolidating the nuclear materials. Indeed, a few weeks ago a DOE task force proposed just that for DOE nuclear weapons research sites, moving all sensitive nuclear materials to a new manufacturing site. What are your views on the report of the task force and have you considered similar consolidation removal of Category I nuclear materials at ESE sites?

Mr. PODONSKY. Again, Mr. Kucinich, from our perspective, from oversight, we think consolidation of nuclear materials is a must for the Department if we are going to change our safeguards posture and if we are going to continue to meet the evolving and potential threat against the Department.

Mr. KUCINICH. It is my understanding, though, if I may, that according to a GAO report, neither ESE nor DOE has developed a comprehensive or coordinated plan. Are we going to see one forthcoming?

Mr. PODONSKY. Again, I am not the program office, but I will attempt to give you an answer from my perspective, and that is that the Secretary of Energy, Secretary Bodman, has in fact put together a nuclear material consolidation task group to take a look at where the possibilities are for consolidation across both ESE sites and NNSA sites. So I have every expectation that, between the two Under Secretaries and the Secretary's focus, that the Department will come up with a plan.

Mr. KUCINICH. I would like to ask the GAO, have you heard any feedback from the Department that they are anticipating bringing a plan to you?

Mr. ALOISE. Not specifically, but we are aware of the task force. We think the plan, again, is what is needed, because we have looked at individual plans and, in some cases, they conflict with each other, site-to-site.

Mr. KUCINICH. OK.

Mr. Friedman, the reaction to your June 2005 report that raised concerns about the excessive oversight of security officers at Y–12, the Oak Ridge, TN facility, was strong. One employee of a contractor, Wackenhut, called your inspectors a bunch of bean counters who didn't understand security practices. Would you care to comment on the reaction by the NRC and Wackenhut officials to the June report? And, also, do you believe security guards are as effective if they work more than 75 hours per week? And is hiring more guards the only solution?

Mr. FRIEDMAN. Mr. Kucinich, I knew three of my grandparents who were immigrants and didn't have a great deal of formal education. They all told me to be the best. Whatever I did, they were satisfied to be the best that I could be. So if I am a good bean counter, I accept that manifold from Wackenhut. And I would rather not comment on it. I think our reports speak for themselves, and I think that comment speaks for itself.

With regard to your second question as I understood it, clearly the Department itself—and this is its criteria, not mine—has said there are a maximum number of hours that a protective force officer can work before they become ineffective. They are just too tired physically. And we found, in a disproportionate number of cases,

that the guards were working beyond the maximum threshold that the Department had established, and the risks, I think, are fairly obvious.

Mr. KUCINICH. Well, they are not obvious. What are the risks?

Mr. FRIEDMAN. The risks are that physically and mentally they are not capable of performing their duties.

Mr. KUCINICH. And what does that mean? Please, help this subcommittee understand what the implications are.

Mr. FRIEDMAN. Well, I think the implications are fairly clear, and that is if the guard force, which is there to protect the facility and protect the material, if the guards are tired, if they are overextended, then I think there is a potential degradation of the security of the facility and the material.

Mr. KUCINICH. So the greater the stress that is put on the guards, the more there is a possibility of a breach of security? Is it possible to say that?

Mr. FRIEDMAN. Well, I am not a physiologist, so I can't speak with authority in that regard, but I think that is the conclusion I would reach, yes.

Mr. KUCINICH. OK.

I guess that is it for now. Thank you, Mr. Chairman.

Mr. TURNER. Mr. Walsh.

Mr. WALSH. Yes, sir.

Mr. TURNER. In your discussion with Chairman Shays——

Mr. WALSH. Yes, sir.

Mr. TURNER [continuing]. I understood your answer to be that you have some disagreement with the current design basis threat based upon available intelligence. And if my understanding is incorrect, could you please tell me what a correct understanding would be?

Mr. WALSH. What I hope to have said was that ESE programs are committed to implementing the design basis threat as provided to us, as it currently stands. We are committed to moving out and doing the things necessary to make sure that we protect against that design basis threat. I think whether or not the——

Mr. TURNER. Let me ask it again. I have to get back to this because your answers concern me because I have a followup question I want to ask you. What I was asking you is the design basis threat a threat that the facilities are experiencing today, is the threat that is out there. And you did not give a yes or no answer, and Chairman Shays said to you, I believe, that one reason why you could not believe that you could give a yes or no answer is if you disagreed with the current design basis threat, that you thought that the current design basis threat was either insufficient or incorrect.

Mr. WALSH. Right.

Mr. TURNER. And I thought I heard you say that you did have some concerns about the current design basis threat.

Mr. WALSH. I said that I was not 100 percent certain, and I believe that it is very important for us to make sure we get that right, we get the DBT right, no matter what it is. But I am not 100 percent certain at this time that the fundamental intelligence that supports and that goes into the process of deciding what the design basis threat is is sufficient, in my mind, that I have seen so far. And there might be other things out there that I haven't

seen. But what I have seen, I am not sure it supports the level that we currently have as what I consider to be the most representative threat against DOE facilities or nuclear facilities in general.

Mr. TURNER. Thank you. Which gets me to my question.

Mr. WALSH. OK.

Mr. TURNER. Do you believe that the current threat is higher or lower than the current design basis threat?

Mr. WALSH. It is very difficult, until we do a more complete review, including a review of all the intelligence that is there. I would really be going out on a limb as to whether I thought it was higher or lower. I would really like to take part in the internal review that we are currently conducting at the request of Deputy Secretary Sell and get that done, and then I will come back and give you a good answer.

Mr. TURNER. Fair answer.

Mr. Friedman, you referenced in your written testimony the non-U.S. citizens that were improperly allowed access to leased facilities at Y–12. Your testimony references it in the plural. Could you tell us how many, if you know?

Mr. FRIEDMAN. Mr. Turner, I know the answer to the question, and it doesn't come to me to recall. It was between 20 and 30.

Mr. TURNER. Non-U.S. citizens——

Mr. FRIEDMAN. That is correct.

Mr. TURNER [continuing]. That used false identification.

Mr. FRIEDMAN. That is right.

Mr. TURNER. Can you say the number again?

Mr. FRIEDMAN. It was about 30.

Mr. TURNER. Dr. Brede, one of the issues that has come up in this hearing as a point to discuss is Wackenhut's foreign ownership. Could you please go over the current foreign ownership structure of Wackenhut and also, if you will, tell us what businesses the parent corporation and affiliate corporations to Wackenhut are engaged in internationally?

Dr. BREDE. Yes, sir. The parent organization is currently British owned. We formed essentially a separate government services organization with a firewall between WSI, which is Wackenhut Services Inc., the government arm of Wackenhut, and the remainder of PWC, or the Wackenhut Corp. In doing so, we went through the FOCI, or foreign owned and controlled process implemented by the Department—not only the Department of Energy, but the Department of Defense—to meet the specific requirements for parent organizations like ours.

We are essentially in the security and emergency services business. We provide firefighting and emergency medical and security services throughout the world.

Mr. TURNER. Mr. Podonsky, in the number of hearings that we have had on these issues, of DOE security, I have always appreciated your forthcoming positions on both concerns and issues where you believe that DOE is performing. And in the materials that we have concerning the GAO report there are a number of references to surveys that have been taken of the officers that are actually providing the security services.

I am just going to review a few of those and then I would like your thoughts on this, because when the GAO sites the issue of mo-

rale, and then when you look at these specific survey statistics, they do not rate well. And I will give even the positive ones and the negative ones.

Specifically, 102 of the 105 officers GAO interviewed say that they believe that they understand what was expected of them. Sixty-five of the 105 officers rated the readiness of their site's protective forces high, while 20 officers rated their protective forces somewhat or moderately ready to defend the site. Only a minority of the officers, 16 of the 105, rated the readiness of their force to defend their sites as low.

Then when you go to the other numbers, when you look at the critique of the force-on-force analysis, 23 of 84 protective force officers that had participated in these exercises believed that they were realistic. While 23 said they were somewhat realistic, in contrast, 38 officers believed they were not realistic.

Then on the communication equipment, 66 of the 105 protective force officers reported that they did not always have dependable radio communications, with 23 officers identifying sporadic battery life, 29 officers reporting poor reception at some locations on the site as the two most important problems.

And when you go to the issue of protective force vehicles, 14 out of 30 of the protective force officers interviewed at two sites reported patrol vehicles were old, in poor physical condition, and not suitable for pursuit and recovery missions.

On the creation of an elite force, 74 out of 105 reported that they are not at all confident in their current ability to defeat the new threats contained in the design basis threat.

Could you comment on the officers' survey responses?

Mr. PODONSKY. The responses from the individuals interviewed by the GAO are often alarming to me in my role in the Office of Oversight and Policy. First and foremost, the elite force, we do believe that the training is important, that we get that to those identified to play that role at their particular sites. Our national training center in Albuquerque, NM is setting up new curricula for that purpose so that we do get the training out to the sites.

In terms of equipment, we have experienced ourselves, during our inspections, that there have been equipment issues, both in protective gear as well as radios, and we have seen that the sites have acknowledged that and are in the process of procuring equipment to fix those issues that were identified.

Relative to the lack of confidence that the force-on-force exercises are realistic, having done force-on-force exercises for my organization for 20 years, I would tell you that the exercises that are our independent oversight runs have a balance between safety and security. But they are as realistic as humanly possible, considering the safety constraints. We don't use real bullets; we use laser.

But we have employed in our organization former Navy Seal Op 6, Delta Force, Army Rangers. We bring people in from real world who—Mr. Shays just came back from the Middle East. We employ people who have served time there so that we can put into place a realistic testing of the forces.

Now, whether the sites, when they do their force-on-force exercise, follow all that same realism, you are probably going to get a mixed story there.

So we don't disagree with the findings or the interviews that the GAO has. We take that on from my policy organization and my oversight organization as the challenge to fix the problems; get out there and find out why the implementation isn't taking place in terms of robust force-on-force. Or, if it is, then let us see how better we can fix it.

Further, make sure that the equipment is provided to the security officers. Obviously, I sit in an interesting situation because we don't implement the policy, we don't fund the equipment; we just criticize what sometimes needs to be criticized, very similar to the Inspector General's Office, but from a different perspective.

But one thing I would also add, the commitment that we have in SSA that I would like this subcommittee to know, we have put in our budget the deployment of new technologies at four sites, both two at NNSA and two at ESE. And the reason we have done that, using money that the Congress has given me for technology deployment and technology development, is to get it out there now and to demonstrate to the program officers that it can be done.

Mr. TURNER. Mr. Chairman. Mr. Kucinich.

Mr. KUCINICH. Thank you very much, Mr. Chairman. And, once again, I want to thank the Chair for calling to the American people's attention some of these very serious security issues. Thank you, Mr. Chairman.

Of course, we are here to talk about what the actions are must be taken that are needed by the DOE to improve security of weapons grade nuclear material at our Energy, Science, and Environmental sites. And it is necessary to focus in on those who are providing the security in order to come to some kind of a conclusion about how secure these sites are. So in that regard I would like to focus some questions on Dr. Brede from Wackenhut, first of all, to kind of get an idea, for those people who aren't as familiar with Wackenhut as certainly you are.

What are Wackenhut's annual sales and their revenue? There was a profit last year. Could you tell us a little bit about the financial strength of the Wackenhut Corp.?

Dr. BREDE. I cannot. I can certainly take that for the record. Initially, in my opening statement, I indicated that I had just come from, as the general manager of the Savannah River site. And I can speak to those financials, but I am not prepared, sir, to address those. However, I am willing to take it for the record.

Mr. KUCINICH. Because I think, as a matter of record, if we have a corporation that is charged with providing security at these sites, we certainly want to know what kind of financial condition that corporation is in. We not only want to know their ownership; we want to know if they are vulnerable to takeover; we want to know if they are making a profit, if they are experiencing a loss; we want to know what their partnerships are. Because we are talking about security, and we have to look at the architecture of security.

Can you tell the subcommittee, Dr. Brede, the security guards who are the subject of some of the discussions here in front of the committee, how much do they make an hour? What is their hourly pay?

Dr. BREDE. It varies. At the Savannah River site they earn something like $19 an hour, with overtime differentials and that sort of thing.

Mr. KUCINICH. That is every security personnel who is working there makes $19 an hour?

Dr. BREDE. No, sir. It is based on—we have unarmed——

Mr. KUCINICH. What is the lowest that a security guard would make?

Dr. BREDE. Somewhere in the range of $12 to $13 an hour.

Mr. KUCINICH. Is the lowest. And do these individuals also have full health benefits?

Dr. BREDE. Yes, they do.

Mr. KUCINICH. And are there any deductibles or co-pays? I mean, is it fully paid health benefits, is that what you are saying?

Dr. BREDE. There are some minor co-pays.

Mr. KUCINICH. And are these people who get paid time and a half for overtime, double time for holidays, and things like that?

Dr. BREDE. Shift differentials, yes, sir.

Mr. KUCINICH. They get that? Are these people who have retirement benefits, do you know?

Dr. BREDE. Essentially, their retirement plan at the Savannah River site is a two-pronged plan. One is there is an annual contribution made to a pension plan and, second, there is a 401(k) matching plan.

One of the things that I pointed out in my opening testimony is that as we build this elite force, one of the things that needs to be looked at is a uniform benefit and retirement plan across the complex, if we are going to effectively recycle human capital through the elite force.

Mr. KUCINICH. And how long have you been with Wackenhut?

Dr. BREDE. I have been with Wackenhut for 12 years, sir.

Mr. KUCINICH. And what about these security guards, do you know generally how long these security guards have been with the Wackenhut Corp.? How long the security guards who are the subject of some of the discussions today, how long they have been with Wackenhut?

Dr. BREDE. I cannot speak to those at other sites. I can say that those at the Savannah River site have been with us anywhere from 21 years, as long as 21 years. More recently I believe our last class was run less than 2 years ago.

Mr. KUCINICH. Because I think it would be instructive for the subcommittee to see what the length of service is of the people that we are talking about so we could be able to make some kind of a determination as to whether or not some of the difficulties that may be experienced at some of these facilities might happen to be with a work force that perhaps is not as well trained.

Now, I would like to ask what is your doctorate in?

Dr. BREDE. It is in criminal justice.

Mr. KUCINICH. Criminal justice, OK. OK, that is important for this next question. What about this issue of guards who are routinely working in excess of 60 hours per week? And that is in direct violation of DOE policy. Do you think that is appropriate?

Dr. BREDE. Actually, what the DOE manual really says is that it imposes a limit of 60 hours, but goes on to say unless there are

alternate arrangements based on collective bargaining agreements between management and the unions, which in the case cited, Oak Ridge, there does happen to be an agreement between the unions there and management.

Mr. KUCINICH. So which unions are you talking about here?

Dr. BREDE. The IGUA and the SFPFA, Security, Police, and Fire Professionals of America.

Mr. KUCINICH. OK. So you are saying you have an agreement with this organization and they say 60 hours is OK. Well, as someone who is a Ph.D. with a background in criminology, do you think having guards working in excess of 60 hours per week is a sound policy?

Dr. BREDE. Our preference would be that they work less than 60 hours a week. However, beginning with the situation we found ourselves in following September 11th, we actually, in some cases, worked much more than that to meet what we perceived as the increased threat. We are hiring additional officers at that particular site, incidentally, to minimize the necessity for overtime.

Mr. KUCINICH. Do you think guards who are working that many hours are as effective as guards who work, let us say, a 40 hour week? What is your experience in that as a criminologist?

Dr. BREDE. Well, I think my more pertinent experience perhaps is my military experience. Are they as effective? I believe the answer is no. But are they sufficiently effective to provide a defense against the threat? I believe they certainly can be based on their training.

Mr. KUCINICH. Well, this subcommittee, at least staff, has provided information that says that these guards are working in excess of 60 hours a week, week after week, month after month. What can you tell this subcommittee about Wackenhut's determination to make sure that these facilities are receiving optimum protection from a work force that is not being ground up?

Dr. BREDE. I would submit to you, sir, that this is not necessarily a Wackenhut issue, but, rather, a protect——

Mr. KUCINICH. Well, let us talk about it in terms of Wackenhut, though.

Dr. BREDE [continuing]. A protective force issue. We are saying we saw the same difficulty across the board at many of our sites following September 11th. One of the problems that we experienced, again, througout the complex, is that when an officer goes through his or her basic training and are employed, we must wait on security clearances.

So there is not an immediate resolution to the overtime problem. We await security clearances and human reliability program clearances before we can always put an officer to work. That does operate to alleviate the problems that we are experiencing with overtime.

Mr. KUCINICH. Well, let me just say this becomes critical to the concerns of this subcommittee about improving security at these nuclear facilities, because if we have a work force that is overextended, that is tired, that doesn't get relief, is working long hours week after week, month after work, you have a work force that is not going to be as alert.

Now, it occurs to me that, notwithstanding Wackenhut's desire to be of service to the United States of America, that it might be, Mr. Chairman, based on the record, that you have an overextended work force here in a contractor who may desperately want to be holding onto a contract, keep working the workers, put in more hours and more hours, but not really be able to meet the terms which we expect to protect. I mean, either you need more people doing it or you need a whole different arrangement that isn't reflected by what Wackenhut is doing, with all due respect.

I have one more question before we move on, and that is for Dr. Adler. Given the number of security problems and other incidents that have been revealed in the last 15 months at DOE facilities guarded by Wackenhut, do you believe that DOE could be better served by hiring a different security contractor or providing security through another kind of protective force or protective force structure? Could you just give us an opinion?

Then I will yield to the chairman.

Dr. ADLER. Thank you very much, Mr. Kucinich. Our comments don't go to the security force structure per se; it goes to the way things are organized at present. No contractor is a saint. Everyone makes mistakes. And if they didn't make mistakes, you wouldn't test. We test to find the mistakes and correct them. The question that I have is what do you do when you find a mistake. Do you admit it honestly? Do you try to discover the roots? Do you attempt to redress the problems and resolve them and move forward?

What we see, however, here is not just a mistake, one or two, a snapshot, as my fellow panel member said. We see something more like a full-length motion picture; and it is not a comedy. What we see here are a series of problems, often on the same themes, that are not being adequately addressed. They are not being adequately addressed by the contractor, nor by those directly responsible for——

Mr. KUCINICH. Well, that is why we are having this hearing.

Dr. ADLER. Yes. And I think the oversight that is being provided by this hearing here is to air these problems.

Let us take, for example, the training issue. There is nothing new in the fact that training is not realistic. The IG made a comprehensive review of this over a year ago and identified training cutbacks and deviations from policy at a number of DOE facilities. We would think that would get people alert, that the practice would be stopped and people would conform with policy or indicate where they are not in conformance.

Well, the IG now reports in June that, in fact, at Y–12 and at Oak Ridge, both facilities, there are deviations from the training. They said in excess of 40 percent of the planned hours are not actually being used for training. Now, why is that the case now? What we would expect is for those careful reports to be acted on and for heads to roll, frankly. For a regime to be set up where there is no tolerance for this sort of behavior, and those who are responsible for it to be appropriately punished so that it is too expensive for them to do it.

Mr. KUCINICH. I want to thank the gentleman.

I want to thank the Chair for his indulgence, and appreciate the committee. Thank you very much.

Mr. TURNER. Mr. Burton.

Mr. BURTON. I understand that this hearing is not about the question that I am going to ask, but maybe somebody can answer it anyhow. And I apologize for my tardiness.

I understand we have 65 nuclear power plants, and I was just told by our staff that there are 103 nuclear reactors. Can anybody tell me what measures are being taken to protect those facilities from either a ground attack or an air attack?

One of the reasons I ask that question is not too long ago, well, twice in the last couple months, we have had scares here in the Capitol, where they had to evacuate the Capitol and other facilities around the Capitol because they thought there might be a plane heading toward the Capitol.

And I would just like to know, with the nuclear exposure we have at these facilities, what measures are being taken to protect those facilities so that if a plane does try to go in there, or they make an attack on one of these power plants, that we don't have a nuclear disaster that spreads nuclear material all over the place.

So anybody that can answer that for me, if you can, I would really appreciate it.

Mr. PODONSKY. Mr. Burton, I don't think any of us could directly answer that question because the facilities you are talking about are licensed under the Nuclear Regulatory Commission. And while we have some relationships with the Nuclear Regulatory Commission, in terms of our exchange on material control accountability, and we are looking at physical security now, I shouldn't speak for everybody, but we could not give you a direct answer.

Mr. BURTON. Who would I address that question to? Does GAO have any information on that? Has GAO looked into that?

Mr. ALOISE. Currently, we do have some work going on now looking at it. We have not finished our work, it is ongoing. NRC has its own DBT, design basis threat, by which it guards its facilities, similar to DOE's design basis threat, although it is not exactly the same.

Mr. BURTON. Maybe I could just ask the chairman, because the chairman is up on all this.

Mr. SHAYS. I would say to the gentleman that what the GAO is doing is a request of ours. Maybe others have requested it as well. We will be having a hearing on the GAO report. We encounter a lot of different issues when we are looking at our nuclear electrical generations plants, whether the security there—for instance, the very people who are defending it also have contracts to try to infiltrate on both sides of the equation, and that is of concern to us. We have a lot of concerns, frankly.

Mr. BURTON. Well, I would like to talk to you about that, because that has been one of my concerns. That is one of the reasons I came down today. Maybe we could do a hearing down the road on that.

Thank you, Mr. Chairman.

Thank you, gentlemen.

Mr. SHAYS. We are almost done here.

We had a hearing one time about whether our troops were exposed to chemical weapons, and we asked the question and DOD said there has been no offensive use of chemicals in Iraq. This was

in the first Gulf war. We then learned and had films of how our troops were exposed in Camassia.

And when we contacted DOD, they came back to us and said, well, our troops hadn't been exposed to offensive use, they were exposed to defensive use. And it made me realize sometimes how you almost get in a word game. I mean, they knew the intent of the subcommittee. And that is why we tend to focus a little bit on how you are answering these questions to understand really what are you saying.

Dr. Brede, when you said that your company is currently owned, you weren't trying to imply that it won't be currently owned in the future? It is in fact owned by——

Dr. BREDE. Absolutely.

Mr. SHAYS. And it just raises the question your people are aware—let me ask you this. Do some of your folks have security clearances or do all of them have security clearances?

Dr. BREDE. The majority of our people do have security clearances.

Mr. SHAYS. And that is because they are in a facility where, if they were on the wrong side of the equation, could do tremendous harm, correct?

Dr. BREDE. Yes.

Mr. SHAYS. So we care greatly about their capabilities. We care about how much they are paid, because we want to make sure you are able to attract good people; people that might want to go somewhere else, but they are paid so well they stay there. Do you have a significant turnover rate?

Dr. BREDE. No. In fact, we do not. At the Savannah River site, for example, the turnover rate there is somewhere in the neighborhood of 2 percent. At the Oak Ridge site, if I may——

Mr. SHAYS. Two percent over what period of time?

Dr. BREDE. Sorry?

Mr. SHAYS. Over what period of time? Is there a time relating to the 2 percent? Two percent means what?

Dr. BREDE. Two percent means we average about 2 percent turnover per year.

Mr. SHAYS. Per year. OK.

Dr. BREDE. And if I recall correctly, at the Oak Ridge site, it is in the neighborhood of 3 to 5 percent. There was an up-tick back in 2001, 2002, where the air marshals were hiring, and some of our officers left to go there. But that has since dissipated and the numbers are much lower now.

Mr. SHAYS. And there is obviously logic to wanting people to have expertise. I mean, if we are training them, to have them leave after they have been trained is not a great use of our resources, or yours.

Dr. BREDE. No, it is not.

Mr. SHAYS. Dr. Adler, your employees work both as government employees and for private contractors, both?

Dr. ADLER. That is correct, sir.

Mr. SHAYS. Do any of them work for Dr. Brede's company?

Dr. ADLER. A small number.

Mr. SHAYS. Is there anything, before this hearing ends, that you would like to add about the employees you represent and the concerns they have?

Dr. ADLER. I think the key point would be that our union has been seeking partnerships with employers, with mayors, Governors, and their clients on consistent ways to raise standards in the security industry, and we have been doing it for a long time. And we do this with the biggest security companies in the country.

The kinds of problems we are talking here today, some of them are large-scale, but the lion's share of them, particularly, I think, around an elite training force, are problems that can come right through consultation with the people involved, if there is a willingness to admit the difficulties and work hard to overcome them.

What I have heard today—and I should say I have heard it from both sides, from the contractors and those responsible—is, to some extent, denial; to another extent I think it is not wishing the problem away, but pretending that the problems have solved themselves. What we have been presented by the GAO and the IG are serious problems. We have encountered these in the private sector, and they are surmountable problems. But it is not a resource problem; the officers aren't poorly paid, and Mr. Podonsky has seconded this. The problem is a matter of will.

Mr. SHAYS. Is what?

Dr. ADLER. The problem is a matter of will, of a willingness to confront these problems and overcome them in consultation with those most directly involved, and in this case I mean the guards. I don't see that emerging from this discussion or from the practices of the Department over the last number of years.

Mr. SHAYS. Is there a difference of approach when the government hires the employees and when the contractor, or is it pretty much similar?

Dr. ADLER. Well, I think the pressure on the private contractor to cut costs is greater than it is in government, particularly if they have to report to a foreign owner who is publicly traded. I think that pressure is there anyway, but I think it is very sharp in the private world. We encounter it all the time in the commercial office world. And those pressures can only be lifted, I think, in an effective regime of oversight that punishes those kinds of cost cuttings.

Mr. SHAYS. GAO has said in their statement, "However, DOE neither sets standards for individual protective force officers participation in these exercises, nor requires sites to track individual participation." This is under the heading "Performance Testing and Training." In your statement it is not that much different, you said "Most officers we spoke with were concerned about their quality and realism of their training," which gets me to your point. "Further, because DOE neither sets standards for nor tracks individual participation for its exercises, it was difficult to determine how many officers had this important training."

I am asking the question why not, and I think it goes to you, Mr. Podonsky, and it goes to you, Mr. Walsh. Why does DOE neither set standards for, nor track individual participation for its exercises? So I will start with Mr. Walsh first.

Mr. WALSH. Mr. Shays, we do need to track that, and we agree 100 percent with those recommendations. We are going to work

with Mr. Podonsky's office. We have already been in contact with each other to commit to develop policy requirements to do that by the end of this year on both of those cases.

Mr. SHAYS. Good. Thank you.

Mr. Podonsky.

Mr. PODONSKY. Mr. Shays, I would tell you candidly I am embarrassed that 17 months ago I took over the policy group and I did not know until the GAO report that the individual tracking of participants in DOE was not taking place. I will tell you that I was under the wrong assumption for 20 years, when my oversight was conducting these tests, that all the sites were tracking and following the performance of each individual. We are changing that.

Mr. SHAYS. That is one reason we have the GAO and an Inspector General, and my attitude is if they point out things that need correction and there is a willingness to jump right in and deal with it, that is when I think the system works the best. We never can make an assumption that they are not going to find things that need work.

So I am happy to end on that note as far as my questions.

Mr. TURNER. Mr. Burton.

Mr. BURTON. First of all, I don't want to belabor this point and discuss something that is not on the agenda today, but about 2½ years ago, I think, according to the staff, you had a hearing on one of the nuclear plants and how they protect them. And according to what your staff expert said was that nuclear plant could withstand an air attack of some magnitude without disbursing a lot of nuclear material into the atmosphere.

I have a television show I do about every couple months, and I had Curt Weldon on, Congressman Weldon, who is an expert in a lot of areas on the National Security Committee. And he brought on a briefcase that the Soviet Union—it was a replica of a briefcase the Soviet Union had made. There were 65 or 70 of them manufactured, and there were nuclear weapons in a briefcase; they weighed about 50 pounds. And I was told by him and other experts that would destroy an area of about five city blocks if it was ever detonated.

Now, several of those briefcase nuclear devices have never been accounted for by the Russians, and there may be others that have been manufactured. So what I would like for GAO to find out is—and I understand from staff that the FAA has some real problems with creating areas around these nuclear power plants where planes can't fly, I guess because of the air lanes that we have.

But it seems to me if a nuclear device can be put in a briefcase, it can certainly be put on a small plane. And if it would destroy five square blocks, it certainly could penetrate and do a lot of damage to a nuclear power plant.

I would like to find out if there is anything we could do to protect those nuclear power plants from that kind of air attack. Because if there is an air attack and you do have something like Chernobyl take place because of that air attack, you are going to have tens of thousands of people dying of radiation poisoning or ancillary diseases, cancer or whatever it happens to be. So I don't know if you guys have ever looked at that at GAO, but I would like—I understand you are doing a research project right now.

Could you include that in your research project? Also, I would like to, in that research project, if you could, there may be some air restrictions by FAA that we could live with, but when you are talking about low-flying aircraft that gets down below, say, 1,000 or 2,000 feet, there might be some way to protect that nuclear facility against that, if it gets within a certain radius that might endanger that area.

There is no question in my mind that small nuclear devices could be produced and put on a small aircraft that could penetrate those, no matter how strong they are, if what I have been told in the past is accurate. And I would just like to find out if there is any way to protect those 60-some nuclear power plants and those 100-some reactors we have from that kind of an attack.

So, Mr. Chairman, I would really like to look into that. And if we could have that study expanded to include that, I would really appreciate it.

Mr. SHAYS. I thank the gentleman. If the gentleman would yield.

Mr. BURTON. I will yield to my colleague.

Mr. SHAYS. My understanding is the NRC is looking at flight zones right now and are looking at the vulnerability. But maybe you could be responsive to the issue, without delving into too much, to say whether, in this mix of looking at the postulated threat and the design basis threat, whether we obviously take a look at aircraft and the possibility of their being able to do damage. Maybe you could respond, someone, to that question.

Mr. PODONSKY. At 1:45 today we are meeting with Deputy Secretary Sell to have the detailed discussion on the latest review of the design basis threat, and part of that is looking at not only the numbers that we have talked about, around, but also in looking at all that encompasses and what kind of threats are realistic today that we really need to protect against.

Mr. SHAYS. Including——

Mr. PODONSKY. Including aircraft and what can we do.

Mr. BURTON. Thank you, Mr. Chairman.

Thank you, gentlemen.

Mr. TURNER. Mr. Friedman, you indicated you wanted to respond?

Mr. FRIEDMAN. I appreciate the courtesy, Mr. Chairman. You asked an important question before about the number of illegal aliens and regarding Y–12, and I misspoke. I wasn't sure that I recalled the answer, and I recalled it incorrectly. The correct answer is 16, and I would like to correct that for the record, if you don't mind. And I thank you and I apologize.

Mr. TURNER. I thank you for that number, and I appreciate your trying to accommodate us with an estimate. So thank you for the correction.

Dr. Brede, Dr. Adler was raising the issue, when we have security that is being provided by a private company, that, unlike in the operations of government-provided security, you have the issue of the bottom line that is more prevalent and, therefore, pressures to cut costs. My thought is that you also have the pressure to increase revenue.

And with the series of questions and concerns that have been raised about the extensive time that some security personnel are

working it made me wonder about the current construct of your contract. The contract under which you are paid for the services, is it a cost-plus contract?

Dr. BREDE. It varies with each site. At Oak Ridge I believe it is a fixed price contract; at the Savannah River site it is a cost plus award fee contract.

Mr. TURNER. And the award fee, is that a percentage of your expenses? Obviously, if you are encouraged to——

Dr. BREDE. It is not a percentage, sir, it is an agreed-upon figure agreed upon at the initiation of the contract, and adjusted based on as missions are added or, in some cases, go away.

Mr. TURNER. OK. Well, for the record, if any of you, Mr. Walsh, Mr. Podonsky, or Dr. Brede, want to supplement the answer, what I am looking for is any financial incentive that you might have as a private contractor to encourage overtime such that the government's expenses go up and therefore your profit goes up, I would be interested in knowing, because it doesn't seem to me, in reading this information about the work week of these security officers, that it makes a whole lot of sense that, certainly, security is not served by officers working in excessive hours.

So I would like to know what else might be at play here. And if there is any increase in revenue to your company as a result of excessive hours of security guards, I would like to know it.

Dr. BREDE. There is not in the two contracts with which I am familiar.

Mr. TURNER. In that, we are going to close, and I will just give everyone an opportunity if there is anything that you want to add to the record before we close.

Mr. PODONSKY. I would, Mr. Chairman. We have talked about the DBT extensively, and I just want to make it clear for the record, from the SSA perspective, that the DBT is in fact the current threat, and it should be met as soon as possible utilizing all the areas that I have talked about previously, to include elite force, training, technology application, nuclear material consolidation, as well as strategies.

And we believe that while we need to meet that as soon as possible, we also recognize hiring new guards, you have to hire cleared guards, and cleared guards take some time. Putting in technology costs some money. But there is no reason in the world that we shouldn't be further along than we are right now.

Dr. BREDE. Yes, I would also offer a statement in closing. Throughout this hearing we have heard allegations of poor performance, of cheating and so on by protective force contractors. I would point out that these have been investigated by the DOE, and refuted in writing and, indeed, in previous testimony by both DOE and contractors. I would submit to you our forces are not perfect. They do make mistakes. But our training is designed so that these human errors are the exception rather than the rule. And I believe their demonstrated performance in competitions, in reviews by Mr. Podonsky's organization prove that out.

Thank you, sir.

Mr. TURNER. I would just like to note, Dr. Brede, I don't think that anyone questioned the individual security officers. I think they questioned the management and the effective management and the

effective providing of resources, which would be your company, and not the individuals who are providing the services. I think the GAO report speaks for itself as to the areas of criticism that it identifies.

Thank you. With that, we will be adjourned.

[Whereupon, at 12:19 p.m., the subcommittee was adjourned.]