HOMELAND SECURITY: MONITORING NUCLEAR POWER PLANT SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

SEPTEMBER 14, 2004

Serial No. 108–265

Printed for the use of the Committee on Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE

98–358 PDF WASHINGTON : 2005

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

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

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

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

BERNARD SANDERS, Vermont (Independent)

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

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

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

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

EX OFFICIO

TOM DAVIS, Virginia
HENRY A. WAXMAN, California

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

CONTENTS

	Page
Hearing held on September 14, 2004	1
Statement of:	
Matthiessen, Alex, Director, Hudson Riverkeeper, Garrison, NY; David Lochbaum, Union of Concerned Scientists, Washington, DC; and Marvin Fertel, vice president and chief nuclear officer, Nuclear Energy Institute, Washington, DC	115
Reyes, Luis, Executive Director of Operations, Nuclear Regulatory Commission, accompanied by Roy P. Zimmerman, Director, Office of Nuclear Security and Incidence Response, Nuclear Regulatory Commission	32
Wells, Jim, Director, Natural Resources and Environment, Government Accountability Office, accompanied by Raymond H. Smith, Jr. Assistant Director; and Kenneth E. Lightner, Jr., Senior Analyst	73
Letters, statements, etc., submitted for the record by:	
Fertel, Marvin, vice president and chief nuclear officer, Nuclear Energy Institute, Washington, DC, prepared statement of	149
Kucinich, Hon. Dennis J., a Representative in Congress from the State of Ohio:	
Letter dated August 18, 2004	30
Letter dated August 19, 2004	22
Prepared statement of	4
Lochbaum, David, Union of Concerned Scientists, Washington, DC, prepared statement of	141
Maloney, Hon. Carolyn B., a Representative in Congress from the State of New York, prepared statement of	13
Matthiessen, Alex, Director, Hudson Riverkeeper, Garrison, NY, prepared statement of	119
Reyes, Luis, Executive Director of Operations, Nuclear Regulatory Commission, prepared statement of	35
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of	19
Wells, Jim, Director, Natural Resources and Environment, Government Accountability Office, prepared statement of	77
Zimmerman, Roy P., Director, Office of Nuclear Security and Incidence Response, Nuclear Regulatory Commission:	
Information concerning force-on-force exercises	110
Information concerning licensee employees	108

HOMELAND SECURITY: MONITORING NUCLEAR POWER PLANT SECURITY

TUESDAY, SEPTEMBER 14, 2004

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

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 2247, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

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

Staff present: Lawrence Halloran, staff director and counsel; J. Vincent Chase, chief investigator; Robert A. Briggs, clerk; Andrew Su, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. SHAYS. A quorum being present, the Subcommittee on National Security, Emerging Threats and International Relations entitled Homeland Security: Monitoring Nuclear Power Plant Security is called to order.

I have a statement. I am going to catch my breath, and I am going to ask the ranking member to start, and then I will make my opening statement.

Mr. KUCINICH. I want to thank the chairman, as always, for his diligence in matters of security in calling these hearings and indicate my appreciation for the attention that you pay to these matters.

Good morning to the Chair and members of the subcommittee and to our witnesses here today. I welcome this opportunity to discuss nuclear security in open session. As both Congress and the public have been stymied for far too long and getting truthful answers to many questions we have about nuclear safety and security.

Three years ago, two incidents shook the faith of the American people in our security. The first, of course, was the tragic attack on our country by terrorists on September 11.

The other less-known incident was the hidden problem going on at the Davis-Besse nuclear reactor in Ohio. These are the facts.

In February 2001 the Nuclear Regulatory Commission began investigating an aging mechanism that often caused cracking in reactors. As a result of these findings in late 2001, the NRC determined that the Davis-Besse plant was at risk and should shut down by December 31, 2001. FirstEnergy, the plant owner, resisted the

order, claiming it should stay open without incident until March 2002. FirstEnergy argued that a shutdown would cause an unnecessary financial burden.

Rather than following its own safety procedures and shutting down Davis-Besse, the NRC relented and allowed the plant to operate until February 2002. After the Davis-Besse plant had been shut down, workers repairing one of five cracked control rod nozzles discovered extensive damage to the reactor vessel head. The workers found a large corroded hole the size of a football in the reactor vessel head next to one of the nozzles. The GAO concluded in a scathing report on May 2004 that the risk estimate used by the NRC to decide whether the plant needed to be shut down was flawed.

The NRC severely underestimated the risk Davis-Besse posed, even exceeding risk levels generally considered acceptable by the Agency. The GAO report shows that the NRC was ill-equipped, ill-informed, and far too slow to react. The NRC's reaction to Davis-Besse was inadequate, irresponsible and left the public at great risk.

The NRC later reported that the plant might have been as close as 60 days to bursting its rust, damaged lid. Fortunately, the health of tens of thousands of Ohio residents was not harmed, but this was a disaster waiting to happen. Let's talk about security.

So, Mr. Chairman, it's very difficult for me to sit here today and to listen without objectivity as the NRC and the nuclear industry lobbyists tell us how much has been spent, how much security has improved in the last 3 years. The facts and independent experts tell us differently.

For example, we know that one security firm, Wackenhut, provides nearly half of the guard forces at our Nation's nuclear sites. Yet, as was documented by the Department of Energy's Inspector General, the report in January of this year questions surround Wackenhut's competency and objectivity to fulfill this crucial mission. The DOE Inspector General found that in simulation attack drills, Wackenhut attackers told the Wackenhut guard defenders the buildings that were being attacked, the targets at those buildings and whether a diversionary tactic would be used.

The IG also noted an industry-funded study found that as many as 50 percent of the guard forces in a New York plant did not meet physical fitness requirements, guards reported for duty drunk, worked 70 to 80 hours per week and were allowed to repeat weapons qualifying tests until they passed them.

In spite of this poor record, and obvious conflict of interest, the commercial industry still decided to hire Wackenhut to provide the attack teams in force-on-force drills at NRC commercial sites. This could be called a case of the fox guarding the hen house and anyone with a shred of common sense—it's a poor decision. It undermined public trust and raises serious questions on who is making the decisions at the NRC. Understandably, the NRC has decided that the less it says the better. It has polled public security information from its Web site. It has restricted public access by public interest groups to information by requiring none disclosure forms or thorough reclassification, even if the information was previously unclassified.

Mr. Chairman, I would like to submit two documents for the record. The first is a letter from Public Citizen to the NRC dated August 19th; and the second is a Freedom of Information Act request submitted by a coalition of public interest groups dated August 18th. Both documents question the rational behind the NRC's announcement in August 2004 that "certain security information formally included in the reactor oversight process will no longer be publicly available and will no longer be updated in the NRC's Web site."

The same information, including performance indicators and physical inspection information, was available on the NRC Web site after September 11. It was temporarily pulled from the Web site for review and returned to it after it was deemed to have no value to potential terrorists.

What has changed to make this information unacceptable for public review? Since the NRC won't hold public hearings, it's up to this subcommittee to find out. Mr. Chairman, we all know that these nuclear plants are decades old and they are decaying. Yet despite the billions of dollars spent to upgrade security at these nuclear plants, the NRC clearly has a long ways to go before it can restore public trust in its position. I have to wonder if an incident such as if this happened at Davis-Besse in Ohio happened today, whether the NRC would tell us about it. The NRC should work to allay public fears about public safety not to foster them. I really look forward to hearing your testimony. Thank you.

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

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

Hearing on "Homeland Security: Monitoring Nuclear Power Plant Security"

September 14, 2004

Good morning, Mr. Chairman, members of the Subcommittee, and to our witnesses here today. I welcome this opportunity to discuss nuclear security in an open session, as both Congress and the public have been stymied for far too long in getting truthful answers to the many questions we have about nuclear safety and security.

Three years ago, two incidents shook the faith of the American people in our security. The first, of course, was the tragic attack on our country by terrorists on 9/11. The other, less-known incident, was the hidden problem ongoing at the Davis-Besse nuclear reactor in Ohio.

These are the facts. In February 2001, the Nuclear Regulatory Commission began investigating an aging mechanism that often caused cracking in reactors. As a result of these findings, in late September 2001, the NRC determined that the Davis-Besse plant was at risk and should shut down by December 31, 2001. FirstEnergy, the plant owner, resisted the order, claiming that it could stay open without incident, until March 2002. FirstEnergy argued that a shutdown would cause an unnecessary financial burden.

Rather than following its own safety procedures and shutting down Davis-Besse, the NRC relented and allowed the plant to operate until February 2002. After the Davis-Besse plant had been shut down, workers repairing one of five-cracked control rod nozzles discovered extensive damage to the reactor vessel head. The workers found a large, corroded hole the size of a football in the reactor vessel head next to one of the nozzles.

GAO concluded in a scathing report in May 2004 that the risk estimate used by the NRC to decide whether the plant needed

to shut down was flawed. The NRC severely underestimated the risk Davis-Besse posed, even exceeding risk levels generally considered acceptable by the agency. The GAO report shows that the NRC was ill equipped, ill informed and far too slow to react. The NRC's reaction to Davis-Besse was inadequate, irresponsible and left the public at grave risk. The NRC later reported that the plant might have been as close as 60 days to bursting its rust-damaged lid. Fortunately, the health of tens of thousands of Ohio residents was unharmed, but this was a disaster just waiting to happen.

So, Mr. Chairman, it is very difficult for me to sit here today and to listen objectively as the NRC and nuclear industry lobbyists tell us how much has been spent, and how much security has improved in the last three years. The facts and the independent experts tell us differently.

For example, we know that one security firm, Wackenhut, provides nearly half of the guard forces at our nation's nuclear sites. Yet, as was documented by the Department of Energy

Inspector General report in January of this year, questions surround Wackenhut's competency and objectivity to fulfill this crucial mission. The DOE IG found that in simulation attack drills, Wackenhut attackers told the Wackenhut guard defenders the buildings that were being attacked, the targets at those buildings, and whether a diversionary tactic would be used. The IG also noted that an industry-funded study found that as many as 50% of the guard forces in a New York plant did not meet physical fitness requirements, guards reported for duty drunk, worked 70 to 80 hours per week, and were allowed to repeat weapons qualifying tests until they passed them.

In spite of this poor record and obvious conflict of interest, the commercial industry still decided to hire Wackenhut to provide the attack teams in force-on-force drills at NRC commercial sites. This is a case of the fox guarding the henhouse, and to anyone with a shred of common sense, it is a poor decision. It undermines public trust, and raises serious questions on who is making the decisions for the NRC.

Understandably, the NRC has decided that the less it says the better. It has pulled public security information from its website, it has restricted access by public interest groups to information by requiring non-disclosure forms or through reclassification, even if that information was previously unclassified.

Mr. Chairman, I would like to submit two documents for the record. The first is a letter from Public Citizen to the NRC dated August 19th and the second is a FOIA request submitted by a coalition of public interest groups dated August 18th. Both documents question the rationale behind the NRC's announcement in August 2004 that "certain security information formerly included in the Reactor Oversight Process will no longer be publicly available, and will no longer be updated on the agency's website."

This same information, including performance indicator and physical inspection information, was available on the NRC website after 9/11. It was temporarily pulled from the website for review, and then returned after it was deemed to have no value to potential

terrorists. What has changed to make this information unacceptable for public review? Since the NRC won't hold public hearings, it is up to this Subcommittee to find out.

Mr. Chairman, we all know that these nuclear plants are decades old and decaying. Yet, despite the billions of dollars spent to upgrade security at these nuclear plants, the NRC clearly has a long way to go before it can restore public trust in it. I have to wonder that if an incident such as that at Davis-Besse in Ohio happened today, whether or not the NRC would even tell us about it. The NRC should work to allay public fears about nuclear safety, not foster them.

Thank you, I look forward to hearing the testimony this morning.

Mr. SHAYS. Thank you, gentlemen. At this time the Chair would recognize Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. Chairman, I want to thank you for your leadership in reviewing the issues of our terrorist attack preparedness, both at our nuclear weapons facilities and our power plants; in your efforts in reviewing our terrorist attack preparedness both of in our nuclear weapons facilities and our power plants; and your efforts in reviewing terrorist attack preparedness of making America's families safer.

The security of nuclear facilities—both weapons facilities and power plants, is an issue this committee has examined through several hearings. In dealing with the security of nuclear weapons facilities, the subcommittee has learned that DOE needs to update its designed basis threat to meet the current security situation, including upgrading equipment, training and its security force.

Our nuclear power plants, though they don't contain weapons, are just as important to protect. They are designed and built to withstand many natural disasters. But we must make sure as a Nation that we do all we can to protect these energy sources from foreseeable attack.

In earlier hearings, we found that DOE has not developed as strong a relationship with DOD in regard to the sharing of resources and information. I look forward from hearing from our witnesses today concerning issues of coordinations of their efforts with DOD and other Federal agencies, and whether they are taking all available steps and precautions to ensure that the proper equipment is available to secure these nuclear power plants.

Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman.

The Chair would recognize Carolyn Maloney.

Mrs. MALONEY. Thank you.

Well, first of all, Chairman Shays, I want like to thank you for your consistent oversight on terrorism and ways to make our country safer. I think you have really done an outstanding job. I thank you on behalf of my constituents.

I would like to welcome all of our witnesses, particularly Mr. Alex Matthiessen, director of the Hudson Riverkeeper from the State of New York.

The purpose of this hearing is to discuss how adequate are the security measures recommended by the Nuclear Regulatory Commission to protect power plants from terrorist attacks. We know that since September 11, there have been some positive steps, but 3 years later, many still have serious and well-founded concerns about the safety of our nuclear power plants. Required preparations for attacks are specified in the classified design basis threat, the DBT. And a new DBT for nuclear plants is set to be implemented by the end of next month by updating requirements are welcomed. There are several concerns about the thoroughness and implementation of the DBT.

One of the greatest concerns is that these new security requirements do not include an analysis on the impact of an attack similar to the one on the World Trade Center. The NRC has announced

that this review is underway, but no analysis has been completed. This is 3 years later, and I want to know why.

I absolutely do not understand why it has not been done when we know that after the September 11 attacks and after the 9/11 Commission reported, that on the list of initial targets proposed by al Qaeda leaders, included planes attacking and flying into nuclear power plants. Khalid Shaikh Mohammed recommended that, and that's spelled out in the 9/11 Commission report.

I would like to hear from our witnesses on the status this analysis. It's a very serious threat to our country. Not only does this plan not include the threat of an aviation attack. The GAO found that it will take several more years before the NRC will have assurances that the plants are protected against the terrorist threats—included in the new DBT—and they will not have detailed knowledge about security at individual facilities to insure that these plants provide the protections included in the DBT.

My understanding, based on the submitted testimony of the GAO, that this is caused because the NRC's review of the new security plans has been rushed largely superficial and because the NRC reviewers are not visiting the plants to obtain details about the plants and view how they work with the plants facilities.

Additionally, I am told it will take up to 3 years for the NRC to test implementation of all the new plans through the force-on-force exercises. And I would like to hear more from the witnesses on these shortcomings.

Regarding the force-on-force exercises, I am interested to hear from the NRC and the Nuclear Energy Institute on the implementation of these exercises.

Earlier this year NEI chose Wackenhut security to provide the attack teams in the force-on-force drills at NRC commercial sites. And we just heard from Mr. Kucinich, an outline of many of the problems there. They did provide security at Indian Point No. 2 nuclear power plant, which is less than 35 miles from the district that I represent.

The utility Interenergy, that had recently acquired the plant, hired a consultant to conduct a probe of security at the facility and found Wackenhut lacking dramatically. I have a list of problems they had. Only 19 percent of the security officers stated that they could adequately defend the plant. And I would like to place all of them in the record.

But they have not improved from there, and Interenergy subsequently terminated Wackenhut's contract as a result of their findings. I would like to put the findings in the record to save time——

Additionally, Wackenhut provides security for close to half of all of the nuclear power plants now. And by allowing them to provide the attack teams on a company with a troubling record will be basically having Wackenhut police themselves—and I refer again to the testimony of Mr. Kucinich—where they were telling them where they were going to attack and etc.

So I think that this is worse than the so-called fox guarding the hen house that Mr. Kucinich referenced. It is not an apparent conflict of interest, but a blatant conflict of interest. And they definitely should not be the ones doing the attack.

Finally, the testimony submitted by GAO states, and it was very, very troubling, "the NRC does not plan to make improvement to their inspection program that GAO previously recommended and still believes is absolutely necessary. So first of all, I want to know why they are not going to make the improvements that GAO recommended. For example, NRC is not following up to verify that all violations of security requirements are corrected."

And I would like an explanation from the NRC on this important question, and why they do not plan to follow some of the recommendations that the GAO believes is so necessary. So I thank the chairman for this oversight hearing. It's important and I yield back the balance of my time.

[The prepared statement of Hon. Carolyn B. Maloney follows:]

Statement of Congresswoman Carolyn B. Maloney
National Security Subcommittee
Government Reform Committee
Homeland Security: Monitoring Nuclear Power Plant Security\
September 14, 2004
10:00 a.m.
2247 RHOB

Thank you Chairman Shays for holding today's important hearing on Nuclear Power Plant Security.

I would like to welcome our witnesses and I look forward to their testimony. I would particularly like to welcome Mr. Alex Matthiessen, Director, Hudson Riverkeeper, Inc. I am very interested in his testimony on Indian Point.

The purpose of this hearing is to discuss how adequate are the security measures recommended by the Nuclear Regulatory Commission (NRC) to protect power plants from terrorist attacks.

We know that since 9/11 there have been some positive steps, but three years later many still have serious and well founded concerns about the safety of our nuclear power plants.

Required preparations for attacks are specified in the classified design basis threat (DBT).

A new DBT for nuclear plants is set to be implemented by the end of next month, while updated requirements are welcomed, there are several concerns about the thoroughness and implementation of the DBT.

One of my greatest concerns is that these new security requirements do not include an analysis on the impact of an attack similar to the one on the World Trade Center. The NRC has announced that this review is underway, but no analysis has been completed.

I don't understand why this has not been done when it is three years after a similar attack – the 9/11 attacks – and after the 9/11 Commission reported that on the list of initial targets proposed by Al Qaeda leader Khalid Sheikh Mohammad included using planes to attack nuclear power plants. I would like to hear from our witnesses on the status of this analysis.

Not only does this plan not include the threat of an aviation attack, the GAO found that it will take several more years before the NRC will have assurances that the plants are protected against the terrorist threats included in the new DBT and they will not have detailed knowledge about security at individual facilities to ensure that these plants provide the protections included in the DBT.

My understanding, based on the submitted testimony of the GAO, that this is caused because the NRC's review of the new security plans has been rushed and largely superficial and because the NRC reviewers are not visiting the plants to obtain details about the plans and view how they work with the plant's facilities. Additionally, it will take up to 3 years for the NRC to test implementation of all the new plans through force-on-force exercises.

I would like to hear more about these shortcomings from all of our witnesses.

Regarding the force-on-force exercises I am interested to hear from the NRC and the Nuclear Energy

Institute (NEI) on the implementation of these exercises.

Earlier this year the NEI chose Wackenhut Security to provide the attack teams in the force-on-force drills at NRC commercial sites.

According to a letter written by an industry watchdog group, the Project on Government Oversight (POGO), to the NRC between 1986 and 2003, Wackenhut provided security at Indian Point #2 Nuclear Power plant, which is less than 35 miles north of my district in New York City. The utility, Entergy, that had recently acquired the plant, hired a consultant to conduct an internal probe of security at the facility; and found:

- "Only 19 percent of the security officers stated that they could adequately defend the plant."
- Some officers believed that as many as "50 per cent of the force may not be physically able to meet the demands of defending the plant;"
- Wackenhut allowed guards to take their weapons qualifying tests over and over again until they passed;
- Guards told of minimal training, of other guards reporting for duty drunk, of security drills that were carefully staged by Wackenhut to insure that mock attackers would be repelled, and of out of shape guards forced to work 70 to 80 hours or more per week.

Entergy subsequently terminated Wackenhut's contract as a result of the investigation.

Additionally, Wackenhut provides security for close to half of the nuclear power plants. By allowing them to provide the attack teams, a company with a troubling track record will be basically policing themselves. I would like to hear from our witnesses if they believe if this is the best way to ensure these exercises have the maximum efficiency?

I am interested in hearing from the NRC and the NEI on how they are addressing these concerns that are being raised by industry watchdog groups such as POGO that [quote] "This is more than a case of the proverbial fox guarding the henhouse. It is not an apparent conflict of interest -- but a blatant conflict of interest." [unquote]

Finally, the testimony submitted by the GAO states that quote "(the) NRC does not plan to make improvement to their inspection program that GAO previously recommended and still believes and still believes are necessary. For example, NRC is not following up to verify that all violations of security requirements have been corrected..."

I would like an explanation from the NRC why they do not plan to follow some of GAO's recommendations that the GAO still believe are necessary.

Mr. SHAYS. I thank the gentlelady.

At this time the Chair would recognize John Duncan from Tennessee.

Mr. DUNCAN. Thank you, Mr. Chairman.

I remember a few days after the original and horrible events of September 11, I was eating dinner and meeting with several Members of the House. And Congressman Callahan, who at that point was a senior member of the Appropriations Committee, estimated that we would spend—he said over $1½ trillion over the next 5 years on security measures. I thought then that his estimate was extremely high. No one challenged him on it.

But I know that just a couple of months ago, Federal Express—just one company—said they spent an extra $200 million on security that they wouldn't have spent.

After the last hearing on this subject, I sent letters to five Department of Energy laboratories and BWXTY 12 just to ask them how much their security measures had increased. I got back these responses. And a 40 percent increase in security spending on Oak Ridge National Laboratory, a 51 percent increase at the Savannah River National Laboratory, 50 percent increases at Argon and a separate 50 percent increase at BWXTY–12.

In addition, we checked with the Tennessee Valley Authority, and their security spending has gone up by 60 percent since September 11, and that doesn't count $30 million extra that they spent after some Nuclear Regulatory Commission ordered some special measures after April 2003.

Security is very, very important, and I don't know if Congressman Callahan was way off on his $1½ trillion, but there are always companies, there are all kinds of security companies now that have gotten into this market and are doing everything they can to sensationalize and scandalize these matters and exaggerate the problem so that they can make more money.

And I am not saying not do anything with regard to security. But if you stop to think about it, if we do—if Congressman Callahan was anywhere close to being right—that's $1 trillion or $1½ trillion that we are not spending on schools, medical research, highways to cut down on the deaths on our Nation's highways, or many, many other good things, whether you might like libraries, national parks or whatever.

And I think back to former Governor Gilmore of Virginia, who was the chairman of the Commission on Terrorism that the President appointed. After his Commission studied the issue of terrorism, he sent this in a cover letter with their reporting, and Governor Gilmore said there will never be 100 percent guarantee of security for our people, the economy and our society. We must resist the urge to seek total security. It is not achievable and drains our attention from those things that can be accomplished.

I just think that we have to make sure that we take serious steps about security, but we also have to make sure that we don't give terrorists undeserved victories by going totally ridiculously overboard on this and that we don't do it simply because there's some companies out here that want to make some more money.

So, with that, I think it's good to keep holding these hearings to make sure that we do have a reasonable and rational response to some of these problems.

Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman.

At this time the Chair would recognize Mr. Ruppersberger from Maryland.

Mr. RUPPERSBERGER. First, Chairman Shays, I agree with Mrs. Maloney that you have done an excellent job as leader this committee and brings a lot of problems as it relates to national security to the attention of this committee. I just hope that as a body of Congress we can hope implement some of the issues that we have learned in these hearings.

The issue of security with respect to nuclear plants, we know that it's very, very important. Our intelligence shows that al Qaeda clearly has made our nuclear plants a target and that was also confirmed in the 9/11 Commission. Now, one of my areas of concern is, first, the issue of privatization and how we manage privatization. I don't have an issue with privatization. It works sometimes. Other times, it is not necessary when we deal with government.

If you are going to privatize, whether it's Wackenhut's name has been mentioned today or anyone else. If we are going to pay to have someone other than government deal with the issue, we want efficiency and we want accountability.

It seems to me that part of the NRC's responsibility is to hold all privatization, such as Wackenhut, accountable for performance. You read in here that people are coming to work intoxicated or they are not prepared or they don't have the physical standards, that concerns me. That's our fault too as the government or NRC because we have not held them liable.

Now, one of my concerns is the issue of consistency in national policies and the regulation of nuclear power plants. This seems to be some conflict between the NRC regulatory abilities versus the privatized operations of the nuclear and commercial entities themselves.

The security standards have already been changed, for example. We have a new design-based threat. DBT formula, which should be a good thing. The required force-on-force exercises have been increased to once every 3 years instead of every 8 years. That's a good thing. The NRC has also issued more orders regarding augmenting barricades, security forces, patrols and restrict plant access.

The Nuclear Energy Institute has claimed an increase of $16 million per site toward security. Despite these changes, however, the reality of lapses in the security provided by and controlled through private industry remains.

And I believe it will take real partnerships to resolve many of the critical changes we face in protecting nuclear sites. We must work toward resolving this situation without putting undue cost pressure upon the industry itself. I believe we as the government need to do better and working with the nuclear industry regarding threats and intelligence information. We need a true working partnership that provides a more thorough examination of how information is classified by NRC.

We must not compromise secure security for public disclosure, but there must remain a balance for the industry to help keep industries secure these nuclear sites.

Thank you.

Mr. SHAYS. I thank the gentleman.

At this time, Ambassador Watson, you have the floor.

Ms. WATSON. I just want to emphasize our role, Mr. Chairman, as the overseers, and I think that oversight has been lagging in the last session. I thank you for bringing to our attention this subject matter, but we are failing in our responsibility if we don't call in our witnesses, raise the right questions, and be sure they are performing in a responsible way. So thank you so very much.

I think that our national security depends on the protection of our nuclear power plants, and what I have heard thus far in other hearings, tells us we have a lot to be worried about. So I hope that we will get new information in this hearing that will be helpful.

Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentlelady and appreciate her comments as well as all of the other Members.

I would like to put my statement on the record as well and say that 3 years ago, the vulnerability of high-value structures to low-tech attack was seared in our national memory. Images of the collapsing Twin Towers and a smoldering hole in the Pentagon forced an assessment of safeguards and vulnerabilities at other critical facilities, including nuclear power plants.

That assessment prompted some immediate steps by the Nuclear Regulatory Commission, the NRC, to strengthen security at the Nation's 65 reactor sites. Last year, we heard testimony from the NRC, the Government Accountability Office, GAO and others describing post-September 11 efforts to update security policies and practices to meet a dynamic new threat environment. But much of that testimony raised as many questions as were answered about the rigor of the NRC regulatory process, the realism of emergency response planning, the willingness of reactor operators to meet new security mandates and the pace of needed change.

So we asked the GAO to monitor implementation of nuclear counterterrorism enhancements, including some recommended in earlier GAO reviews. Their initial findings depict a lengthy process that risk becoming more theoretical than actual. A new protection standard—or design basis threat—was not issued until April 2003. A rushed review of facility plans implementing the DBT could be completed next month. But that has been formulaic, wholly paper exercise. The NRC will not have complete, site-specific data, from force-on-force exercises to validate upgraded security plants for 3 more years. Even then, there may be no reasonable assurance plants are adequately protected.

Suddenly—I think I am even one of them—the new DBT understates the true level of risk, meaning that security plants will have to be modified and tested again. Despite persistent efforts by reactor operators and regulators to minimize the risks of containment breach or spent fuel sabotage, surrounding communities and those further down wind, take little comfort from a cosy indulgent regulatory process that looks and acts very much like business as usual.

Findings of security violations, illicit promises of, correction, but little NRC followup. Emergency response plans may not be current. Lessons learned are not shared. And a proposal to hire an attacking force from the same company used to protect several plants raises legitimate concerns about the integrity of future mandatory force-on-force exercises. There is no question nuclear power plants remain of abiding interest to terrorists.

However, real questions remain. How and when the seriousness of that threat will be fully reflected in the substance and speed of critical countermeasures.

As we continue to pursue these questions, the subcommittee sincerely appreciates the experience and expertise brought to the discussion by all our witnesses. We look forward to their testimony.

Taking care of some general business, I ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record and that the record remain open for 3 days for that purpose.

Without objection, so ordered.

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

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

TOM DAVIS, VIRGINIA,
CHAIRMAN

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

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

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

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

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

BERNARD SANDERS, VERMONT,
INDEPENDENT

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

Statement of Rep. Christopher Shays
September 14, 2004

Three years ago, the vulnerability of high-value structures to low-tech attack was seared into our national memory. Images of the collapsing Twin Towers and a smoldering hole in the Pentagon forced an assessment of safeguards and vulnerabilities at other critical facilities, including nuclear power plants.

That assessment prompted some immediate steps by the Nuclear Regulatory Commission (NRC) to strengthen security at the nation's sixty-five reactor sites. Last year, we heard testimony from the NRC, the Government Accountability Office (GAO) and others describing post-9/11 efforts to update security policies and practices to meet a dynamic new threat environment. But much of that testimony raised as many questions as were answered about the rigor of the NRC regulatory process, the realism of emergency response planning, the willingness of reactor operators to meet new security mandates, and the pace of needed changes.

So we asked the GAO to monitor implementation of nuclear counter-terrorism enhancements, including some recommended in earlier GAO reviews. Their initial findings depict a lengthy process that risks becoming more theoretical than actual. A new protection standard, or Design Basis Threat (DBT), was not issued until April 2003. A rushed review of facility plans implementing the DBT could be completed next month, but that has been formulaic, wholly paper exercise. The NRC will not have complete, site-specific data from force-on-force exercises to validate upgraded security plans for three more years.

Even then, there may be no reasonable assurance plants are adequately protected. Some believe the new DBT understates the true level of risk, meaning that security plans will have to be modified and tested again.

Despite persistent efforts by reactor operators and regulators to minimize the risks of containment breach or spent fuel sabotage, surrounding communities and those farther downwind take little comfort from a cozy, indulgent regulatory process that looks and acts very much like business as usual. Findings of security violations elicit promises of correction, but little NRC follow-up. Emergency response plans may not be current. Lessons learned are not shared. And a proposal to hire an attacking force from the same company used to protect several plants raises legitimate concerns about the integrity of future mandatory force-on-force exercises.

There is no question nuclear power plants remain of abiding interest to terrorists. Real questions remain how and when the seriousness of that threat will be fully reflected in the substance and speed of critical countermeasures.

As we continue to pursue those questions, the Subcommittee appreciates the experience and expertise brought to the discussion by all our witnesses. We look forward to their testimony.

Mr. KUCINICH. Mr. Chairman.

Mr. SHAYS. Yes.

Mr. KUCINICH. These are the letters I would ask to be entered into the record.

Mr. SHAYS. This is from the Union of Concerned Scientists without objection dated August 19th. We will add that to the record.

[The information referred to follows:]

Union of Concerned Scientists

Citizens and Scientists for Environmental Solutions

August 19, 2004

Chief - FOIA-LPDR Branch
Division of Freedom of Information and Publication Services
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: FREEDOM OF INFORMATION ACT REQUEST

Good Day:

Pursuant to the Freedom of Information Act, 5 U.S.C. 552, as amended and 10 C.F.R. 9.8 of the Commission's regulations, and on behalf of Citizens Awareness Network (CAN), Committee to Bridge the Gap (CBG), EFMR Monitoring Group (EFMR), Friends of the Coast Opposing Nuclear Pollution, Greenpeace, Mothers for Peace (M4P), North Carolina Waste Awareness and Reduction Network (NC WARN), Nuclear Control Institute (NCI), Nuclear Information and Resource Service (NIRS), Public Citizen, Riverkeeper, Three Mile Island Alert (TMIA), and the Union of Concerned Scientists (UCS), I hereby request all "documents" in the possession of the NRC, including but not limited to all regional and headquarters offices, the office of the Executive Director of Operations, the NRC Chairman and all Commissioner's offices, the office of Nuclear Security and Incident Response, and "documents" between the agency and the Nuclear Energy Institute and/or the industry's Security Working Group, related to the deliberative processes and bases for three agency decisions:

1. Decision made prior to the nationwide implementation of the revised reactor oversight process in April 2000[1] that performance indicator (PI) and NRC inspection information for the physical protection cornerstone be made publicly available.

2. Decision made following the tragic events of 09/11 that performance indicator and NRC inspection information for the physical protection cornerstone can again be made publicly available.[2]

3. Decision made prior to August 4, 2004, to remove performance indicator and NRC inspection information for the physical protection cornerstone from the public arena.[3]

---

[1] Nuclear Regulatory Commission, News Release No. 00-055, "NRC To Expand Use of Revised Reactor Oversight Process," March 29, 2000.
[2] Nuclear Regulatory Commission, News Release No. 01-124, "Threat to Three Mile Island Nuclear Plant Deemed Non-Credible; NRC Monitoring Continues and Website Restored," October 18, 2001.
[3] Nuclear Regulatory Commission, News Release No. 04-091, "NRC Modifies Availability of Security Information," August 4, 2004.

Washington Office: 1707 H Street NW Suite 600 • Washington DC 20006-3919 • 202-223-6133 • FAX: 202-223-6162
Cambridge Headquarters: Two Brattle Square • Cambridge MA 02238-9105 • 617-547-5552 • FAX: 617-864-9405
California Office: 2397 Shattuck Avenue Suite 203 • Berkeley CA 94704-1567 • 510-843-1872 • FAX: 510-843-3785

Please note that we are not seeking performance indicator and/or NRC inspection finding information via this FOIA request. We are narrowly seeking information in "documents" about the agency's decisions whether this information should be made publicly available. Please consider "documents" to include reports, studies, test results, correspondence, memoranda, meeting notes, meeting minutes, working papers, graphs, charts, diagrams, notes and summaries of conversations and interviews, computer records, e-mail and any other form of written communications including internal NRC memoranda.

We realize that it is uncommon, if not unprecedented, for the NRC to receive a FOIA request from such a large coalition of public interest groups. We opted for a group FOIA request to clearly convey to the NRC how important this matter is to us and because each of our organizations is very interested in the information contained within the requested records.

Pursuant to and in compliance with NRC regulations at 10 CFR 9.41, we request that any searching and copying fees incurred as a result of this search be waived, and provide the following information in response to the eight criteria listed in Section 9.41(b):

1. **Purpose of request**

   We seek to understand decisions made by the NRC about the public availability of information relative to the NRC's reactor oversight process and the physical protection (i.e., nuclear plant security) component of that process. When the revised reactor oversight process was being developed, there was considerable deliberation about the appropriate amount of information to make publicly available leading to an agency decision that the performance indicator and NRC inspection finding data would be publicly released. After the tragic events of 09/11, the NRC temporarily closed its website and revisited the issue of public access to agency information. After considerable deliberation in that new light, an agency decision was made to resume the release of performance indicator and NRC inspection finding data to the public. In 2004, another agency decision was made that reversed the two prior decisions and resulted in all this information being removed from the public arena. The purpose of our request to more fully understand the bases for these three decisions in proper context.

   A secondary purpose for this request is to enable us to better understand the NRC's policy on security information that can be freely discussed publicly. We all possess information on nuclear plant security obtained prior to 09/11 and/or prior to the NRC's August 4, 2004, announcement. Security information posted on the NRC's website or reasonably deemed less exploitable than security information posted on the NRC's website was clearly available for public discussion. We seek to better understand the agency's recent decision so we can continue to provide responsible public commentary on this important subject without inadvertently divulging "sensitive information [that] might be misused by those who wish us harm" to quote NRC Chairman Nils Diaz.[4]

2. **Extent to which we will extract and analyze the substantive content of the records**

   We seek to better understand how the issue of what information about nuclear plant security can responsibly be made public could be carefully considered twice by the NRC – once shortly before and once immediately after 09/11 – with a consensus on performance indicator and inspection finding data and subsequently reversed years later. We seek to understand what factors were considered in these three decisions and if new factors or re-weighting of old factors accounted for the different outcomes.

---

[4] Nuclear Regulatory Commission, News Release No. 04-091, "NRC Modifies Availability of Security Information," August 4, 2004.

3. **Nature of the specific activity or research in which the records will be used and our qualifications to utilize the information for the intended use in such a way that it will contribute to public understanding**

Our group has a long history of involvement on this matter. For example, UCS was heavily engaged during the development and implementation of the revised reactor oversight program. UCS served on the Pilot Program Evaluation Panel, a group chartered by the NRC in accordance with the Federal Advisory Committee Act to monitor the pilot program period for the reactor oversight program and comment on it. In addition, UCS made several presentations to the NRC Commission regarding the reactor oversight program's strengths and weaknesses. And UCS provided formal comments to the NRC every year since the reactor oversight process was implemented during the agency's annual assessment effort. Before and after 09/11, UCS identified security information on the NRC's website and in ADAMS that appeared too sensitive for public consumption. Prior to 09/11, NCI, NIRS, Public Citizen, and UCS participated in NRC public meetings conducted approximately monthly on the NRC's security program. This involvement included reviewing and commenting on the interim physical protection significance determination process used to assess the significance of NRC findings from security inspections. Friends of the Coast has engaged the NRC on security issues at Maine Yankee since 1998. Since 09/11, all of us have been deeply involved in nuclear plant security issues including testifying before the U.S. Congress and updating our members and citizens about security matters. Many of our organizations have submitted petitions to the NRC under 10 CFR 2.206 seeking security upgrades, such as the 2002 petition by Friends of the Coast on the independent spent fuel storage installation at Maine Yankee. NCI and POGO were solicited by the NRC to speak on security issues at the agency's annual Regulatory Information Conference. And we were invited by the NRC to and we participated in its public meeting on August 4, 2004, where the latest decision was announced.

We seek the requested information to further our understanding and awareness of the reactor oversight process, specifically the physical protection component of it. As representatives of public interest groups, acquiring this understanding and awareness will enable us to better represent the public's interests before the NRC, Congress, the media, and our members.

4. **Likely impact on the public's understanding of the subject as compared to the level of understanding of the subject prior to disclosure**

There have been three decisions by the NRC since January 2000 on the same question: should performance indicator and NRC inspection finding information for the physical protection cornerstone be publicly available? Two decisions, including one made shortly after and in direct response to 09/11, were "yes" and one decision was "no." There's considerable public understanding of the deliberative process leading up to the first "yes" decision because that process included numerous public meetings. There's some public understanding of the deliberative process leading up to the second "yes" decision based on records previously obtained from the agency under the FOIA. There's essentially no public understanding of the deliberative process leading up to the third decision. The information we are requested will greatly increase the public's understanding of all three decisions.

5. **Size and nature of the public to whose understanding a contribution will be made**

Collectively, the organizations joined in this FOIA request have membership in the tens of thousands. Our membership is diverse in terms of age, geographic location, occupation, and other factors but generally aligned about responsible stewardship of the environment. Additionally, we reach many other persons via our media work, Capitol Hill work, and materials posted on our websites

(www.tmia.com, www.nukebusters.org, www.cfmr.org, www.ncwarn.org, www.nci.org, www.citizen.org, www.nirs.org, www.riverkeeper.org, www.mothersforpeace.org, www.greenpeace.org, and www.ucsusa.org).

6. Means of distribution of the requested information

We will incorporate insights obtained from the requested information in presentations to the NRC Commission and during other NRC public meetings, such as at next year's Regulatory Information Conference (RIC) and at the next public meeting on nuclear plant security. We will also use the insights during interviews with the media and in testimonies before the U.S. Congress.

7. Whether free access to information will be provided

Yes.

8. Commercial interest by any party to this request?

No.

If all or any part of this request is denied, please cite the specific exemptions relied upon in refusing to release the materials. Further, since the Freedom of Information Act provides that the remainder of a file must be released if only portions are exempt from disclosure, we request that we be provided with all non-exempt portions that are reasonably degradable. Of course, we reserve the right to appeal the withholding or deletion of any information.

If the NRC provides the requested "documents" to UCS, UCS will ensure copies are provided to the co-requesters.

Sincerely,

David Lochbaum
Nuclear Safety Engineer
Union of Concerned Scientists
1707 H Street NW, Suite 600
Washington, DC 20006-3919
(202) 223-6133
(202) 223-6162 fax

Co-requesters (arranged by organization name in alphabetical order):

Deb Katz
Citizens Awareness Network

Dan Hirsch
Committee to Bridge the Gap

Eric Epstein
EFMR Monitoring Group

Ray Shadis
Friends of the Coast Opposing Nuclear Pollution

Jim Riccio
Greenpeace

Rochelle Becker
Mothers for Peace

Jim Warren
NC WARN

Paul Leventhal
Nuclear Control Institute

Paul Gunter
Nuclear Information and Resource Service

Wenonah Hauter
Public Citizen

Kyle Rabin
Riverkeeper

Scott D. Portzline
TMI Alert

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

In the Matter of	)	
	)	
DUKE ENERGY CORPORATION	)	Docket Nos. 50-413-OLA
	)	50-414-OLA
(Catawba Nuclear Station, Units 1 and 2)	)	

CERTIFICATE OF SERVICE

I hereby certify that copies of the foregoing COMMISSION MEMORANDUM AND ORDER (CLI-04-21) have been served upon the following persons by U.S. mail, first class, or through NRC internal distribution with copies by electronic mail as indicated.

Office of Commission Appellate
Adjudication
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Administrative Judge
Ann Marshall Young, Chair
Atomic Safety and Licensing Board Panel
Mail Stop - T-3 F23
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: amy@nrc.gov

Administrative Judge
Anthony J. Baratta
Atomic Safety and Licensing Board Panel
Mail Stop - T-3 F23
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: ajb5@nrc.gov

Administrative Judge
Thomas S. Elleman
Atomic Safety and Licensing Board Panel
5207 Creedmoor Rd., #101
Raleigh, NC 27612
E-mail: elleman@eos.ncsu.edu

Susan L. Uttal, Esq.
Antonio Fernández, Esq.
Margaret J. Bupp, Esq.
Office of the General Counsel
Mail Stop - O-15 D21
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: slu@nrc.gov; axf2@nrc.gov; mjb5@nrc.gov

Henry B. Barron, Executive Vice President
Nuclear Operations
Duke Energy Corporation
526 South Church Street
P.O. Box 1006
Charlotte, NC 28201-1006
E-mail: hbarron@duke-energy.com

Mary Olson
Director of the Southeast Office
Nuclear Information and Resource Service
729 Haywood Road, 1-A
P.O. Box 7586
Asheville, NC 28802
E-mail: nirs@main.nc.us

Diane Curran, Esq.
Harmon, Curran, Spielberg
& Eisenberg, L.L.P.
1726 M Street, NW, Suite 600
Washington, DC 20036
E-mail: dcurran@harmoncurran.com

Docket Nos. 50-413-OLA and 50-414-OLA
COMMISSION MEMORANDUM AND ORDER
(CLI-04-21)

David A. Repka, Esq.
Anne W. Cottingham, Esq.
Mark J. Wetterhahn, Esq.
Winston & Strawn LLP
1400 L Street, NW
Washington, DC 20005
E-mail: drepka@winston.com;
acotting@winston.com;
mwetterh@winston.com

Lisa F. Vaughn, Esq.
Duke Energy Corporation
Mail Code - PB05E
422 South Church Street
P.O. Box 1244
Charlotte, NC 28201-1244
E-mail: lfvaughn@duke-energy.com

Paul Gunter
Nuclear Information and Resource Service
1424 16th St., NW, Suite 404
Washington, DC 20036
E-mail: pgunter@nirs.org

Timika Shafeek-Horton, Esq.
Duke Energy Corporation
Mail Code - PB05E
422 South Church Street
Charlotte, NC 28242
E-mail: tshafeek@duke-energy.com

[Original signed by Evangeline S. Ngbea]

Office of the Secretary of the Commission

Dated at Rockville, Maryland,
this 29th day of July 2004

Mr. KUCINICH. There is a letter right behind the it.

Mr. SHAYS. There is a letter right behind it. Let's get that one.

Mr. SHAYS. And then a letter from Public Citizen dated August 18th. Both will be put in the record and without objection so ordered.

[The information referred to follows:]

Buyers Up • Congress Watch • Critical Mass • Global Trade Watch • Health Research Group • Litigation Group
Joan Claybrook, President

August 18, 2004

Steven R. Stein
Room 4 F22, Mail Stop 4 D8
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Ronald K. Frahm, Jr.
Room 7 C7, Mail Stop 7 A15
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Dear Mr. Stein and Mr. Frahm:

As you know, your agency announced on August 4 of this year its determination "that certain security information formerly included in the Reactor Oversight Process will no longer be publicly available, and will no longer be updated on the agency's website."[1] This decision took many people by surprise, especially since such information has previously been reviewed at least twice—both before and in the immediate aftermath of September 11, 2001—in the context of its usefulness in the hands of terrorists.[2] In both cases it was apparently determined that the type of information being released was safe for public dissemination and posed no security threat.

As a public interest organization representing almost 160,000 members nation-wide, we have a 30-year history of not only fighting for adequate nuclear plant safety and security measures, but for principles of open government and citizen empowerment in general. Pursuant to our mission, and while recognizing the need to balance security with openness, we have concerns that the recent policy change could significantly impair the ability of the public to provide crucial oversight of nuclear security matters without appreciably improving plant security. Hence, Public Citizen asks six questions to which we respectfully request answers:

1. What act(s) or information prompted a review of the Reactor Oversight Process that led to this determination?

---

[1] Press Release, U.S. Nuclear Regulatory Commission; August 4, 2004; http://www.nrc.gov/reading-rm/doc-collections/news/2004/04-091.html.
[2] "Recommendations for Reactor Oversight Process Improvements," U.S. Nuclear Regulatory Commission; http://www.nrc.gov/reading-rm/doc-collections/commission/secys/1999/secy1999-007/1999-007ascy.pdf; Attachment 1, p. 4, response J; Public Citizen commented on the changes at the time. Much discussion during this process focused on the usefulness of such information to enemies of the United States. Also, on October 17, 2001, NRC shut down its website to review all information in light of the September 11 attacks, and subsequently reposted physical protection data.

2. What authority does NRC have to unilaterally determine what information does and does not pose a security threat and what is therefore suitable for public release? Are such decisions subject to appeal?

3. What oversight mechanisms exist for reviewing NRC's security-related information decisions? Have they been followed?

4. Has the information no longer available been classified? If not, what designation has it been given that prevents its public release? Who made that determination?

5. What specifically are NRC's plans to keep the public informed on the status of security at nuclear power plants?

6. Please clarify: when you state that certain security information will no longer be updated on the agency's website, does this mean previously posted material will remain available or that affected information will be removed? Is information that may have been removed still considered publicly available or has it been retroactively classified or otherwise designated not suitable for public dissemination?

Your timely response to these questions, as well as any other information that may shed more light on the recent decision, would be much appreciated. If you have any questions, please contact Brendan Hoffman of my staff at (202) 454-5130 or bhoffman@citizen.org.

Sincerely,

/s/

Wenonah Hauter
Director, Critical Mass Energy and Environment Program

CC: Andrew H. Card, Jr.
Assistant to the President and Chief of Staff
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500
Fax: (202) 456-2461

Attorney General John Ashcroft
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530-0001
Fax: (202) 307-6777

Matthew W. Stephan
Policy Analyst, Liaison to U.S. NRC
Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue NW, Room 500
Washington, DC 20408
Fax: (202) 219-5385

The Honorable Edward Markey
2108 RHOB
U.S. House of Representatives
Washington, DC 20515
Fax: (202) 226-0092

Mr. SHAYS. We have and we are grateful to have our first panel, Mr. Luis Reyes, executive director of operations of the Nuclear Regulatory Commission and Mr. Roy P. Zimmerman, director, Office of Nuclear Security and Incidence Response, Nuclear Regulatory Commission.

What we are going to do is we are going to have them make their statements. We will go through a 5-minute round of questioning. We are then going to have the GAO make their statement, ask them questions and then do a second round to our first panel separately afterwards. We appreciate our first panel being willing to do it. It's to everyone's advantage to have that kind of dialog, and that makes me feel good that you recognize that and I appreciate it.

So with that, we would ask you to stand and swear you in as we swear all our witnesses.

[Witnesses sworn.]

Mr. SHAYS. Note for the record our witnesses are responding in the affirmative. Is there anyone I should have asked in your staff that may need to respond? If so, it may make sense for me to swear them in.

Mr. REYES. No, Roy and myself are the ones doing the testimony.

Mr. SHAYS. OK. That's fine. That's great.

With that, Mr. Reyes, you have the floor and am happy to have with your statement.

STATEMENTS OF LUIS REYES, EXECUTIVE DIRECTOR OF OPERATIONS, NUCLEAR REGULATORY COMMISSION, ACCOMPANIED BY ROY P. ZIMMERMAN, DIRECTOR, OFFICE OF NUCLEAR SECURITY AND INCIDENCE RESPONSE, NUCLEAR REGULATORY COMMISSION

Mr. REYES. Thank you.

Mr. Chairman, members of the subcommittee, it is indeed a pleasure to appear before you today to discuss some of the efforts by the Nuclear Regulatory Commission.

Mr. SHAYS. I am going to have you move that mic a little more in direct line with you.

Mr. REYES. OK. Is that any better?

Mr. SHAYS. Yes. Just turn it this way. Thank you.

Mr. REYES. To the efforts by the Nuclear Regulatory Commission and its licensees with respect to security at nuclear power plants. The NRC has greatly enhanced requirements of licensees at nuclear power plants and conducted vulnerability assessments and identified mitigation strategies in order to improve security and evaluate potential threats. Nuclear power plants have maintained a strong safety and security measures and were designed to withstand catastrophic events including fire, flood, earthquakes and tornados.

Security at nuclear facilities across the country has long been the subject of NRC regulatory oversight, dating back to the 1970's. And nuclear power plants have been required to implement security problems that are capable of defending against violent assault by well-armed, well-trained adversaries.

Nuclear power facilities have likely been among the best protected commercial facilities in the Nation prior to September 11, 2001 and remain so today. However, the September 11th terrorist

attacks on the United States brought to light a new and more immediate threat to our country.

To cope with these changes in the threat environment, the NRC undertook a reassessment of its safeguards and security programs to identify from actions, and long-term enhancements that will raise the level of security at the nuclear facilities across the country.

Since the terrorist attacks, the NRC has ordered as licensee to take specific actions to security at their facilities and to amend the protection of the nuclear materials they possess. We believe that this comprehensive act also effectively addressed major congressional concerns about the adequacy of security in the new threat environment. We recognize though that security would be further enhanced in the five legislative proposals that the Commission has submitted to Congress which are appended to our testimony are promptly enacted.

My full statement submitted for the record provides a summary of the numerous post-September 11 actions and enhancement to raise the level of security at nuclear facilities.

This includes a series of orders through all nuclear power licensees beginning in February 2002 to formally incorporate specific compensatory measures into the search safeguards and security programs. This enhancement of security included increased security patrols, augmented security forces, additional security posts, increased vehicle span of distances and improved coordination with law enforcement.

In the months since those orders were issued, there has been coordination with the regulated industry and representatives of the Federal, State and local government agencies that would be called upon to support the licensees response to a potential terrorist attack.

Also, following the September 11, 2001 attacks, the NRC began a reassessment of the design basis threat [DBT]. As a result, the threat characteristic set forth in NRC regulations were supplemented by orders issued to power reactors and to certain field cycle facilities.

The NRC's currently reviewing licensee revised security plants for nuclear power plants and certain nuclear fuel facilities. Nearly 2,000 plants in all, and expects that all the plants will be reviewed, revised as appropriate and approved, and with few exceptions implemented by October 29, 2004 deadline imposed by the Commission's April 29, 2003 orders.

Additionally, the NRC has completed an extensive set of vulnerability assessments and identified mitigation strategies for NRC license activities involving radioactive materials and nuclear facilities. These efforts have continued to affirm the robustness of the effectiveness of these facilities, the effectiveness of redundant systems and defense of design principles and the value of effective programs for operator training and emergency preparedness.

We have continued to improve our security performance evaluation program, that is our force-on-force evaluations.

In February 2004 the NRC began a transition force-on-force program incorporating lessons learned during the pilot. The transition program uses the characteristics of the DBT as enhanced as sup-

plemented by our orders to prepare for resumption of the full security performance assessment program in November 2004.

In conclusion, my full statement also includes prescriptions of NRC's revised base line inspection program, the status of security plan reviews, emergency preparedness and sharing of information with our stakeholders.

I appreciate the opportunity to appear before you today. And I look forward to answering any questions you may have.

[The prepared statement of Mr. Reyes follows:]

STATEMENT SUBMITTED

BY THE

UNITED STATES NUCLEAR REGULATORY COMMISSION

TO THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS

COMMITTEE ON GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

HOMELAND SECURITY: MONITORING NUCLEAR POWER PLANT SECURITY

SUBMITTED BY

LUIS A. REYES
EXECUTIVE DIRECTOR FOR OPERATIONS

Submitted: September 14, 2004

Introduction

Mr. Chairman and Members of the Subcommittee, it is a pleasure to appear before you today to discuss some of the efforts by the Nuclear Regulatory Commission (NRC) and its licensees with respect to security at nuclear power plants.

Overview

The NRC's mission is to regulate nuclear reactors, materials and waste facilities in a manner that protects the health and safety of the public, promotes the common defense and security, and protects the environment. Nuclear power plants have maintained strong safety and security measures, and were designed to withstand catastrophic events including fire, flood, earthquakes, and tornadoes. These plants were also designed using a defense-in-depth strategy, with redundant safety systems and are operated and protected by highly trained staff. Multiple barriers protect the reactor and prevent or mitigate off-site releases of radioactive materials. Design features of the reactor facilities provide substantial protection against a malevolent attack.

Security at nuclear facilities across the country has long been the subject of NRC regulatory oversight, dating back to the 1970's, and nuclear power plants have been required to implement security programs that are capable of defending against violent assaults by well-armed, well-trained adversaries. With sophisticated surveillance equipment, stringent access controls, physical barriers, professional security forces, and well qualified armed response forces and partnership with the local law enforcement agencies (LLEA), the nuclear power

facilities have likely been among the best protected commercial facilities in the Nation prior to September 11, 2001, and remain so today. Coupled with emergency plans that are tested on a regular basis and support from local government agencies, these facilities are designed, operated, and regulated to protect the public from a wide range of events, including potential terrorist attacks.

The terrorist attacks on the United States brought to light a new and more immediate threat to our country. All custodians of the Nation's critical infrastructure needed to reconsider decisions made earlier about the adequacy of security at the facilities under their charge. To cope with these changes in the threat environment, the NRC undertook a reassessment of its safeguards and security programs, to identify prompt actions and long-term enhancements that would raise the level of security at the nuclear facilities across the country.

Since the terrorists attacks, the NRC has ordered its licensees to take specific actions to improve security at their facilities and to augment the protection of the nuclear materials they possess. Additionally, we have made internal programmatic and organizational changes to enhance the effectiveness of NRC's regulation of the security of nuclear facilities and materials. We believe that these comprehensive acts also effectively address major congressional concerns about the adequacy of security in the new threat environment. We recognize though that security would be further enhanced if five legislative proposals that the Commission has submitted to the Congress, which we discuss later in this testimony, are promptly enacted.

Orders

In the weeks and months following September 11, the NRC focused its efforts on improving security at the facilities and activities it regulates, including nuclear power plants, Category I fuel cycle facilities possessing significant quantities of special nuclear material, and transportation of spent nuclear fuel. Compensatory measures were imposed and the NRC required licensees to make changes to their security programs to deal with a new level of threat.

On February 25, 2002, the NRC issued Orders to all nuclear power plant licensees requiring that they formally incorporate specific compensatory measures into their safeguards and security programs. These enhancements to security included increased security patrols, augmented security forces, additional security posts, increased vehicle standoff distances, and improved coordination with law enforcement. On January 7, 2003, another set of Orders, designed to enhance security by tightening the plant access authorization requirements, was issued. On April 29, 2003, the NRC issued additional Orders setting security officer work-hours limitations to minimize fatigue; new training and qualification requirements for security force members; and requiring licensees to revise their security and contingency plans to protect against a new level of threat.

In the months since those Orders were issued, there has been close coordination with the regulated industry and representatives of Federal, State, and local government agencies that would be called upon to support the licensees' response to a potential terrorist attack. The Orders of April 2003 required that the licensees submit their revised security plans to the NRC by April 29, 2004, for review, revision as appropriate, and approval. The NRC staff is on schedule to complete its review of these plans and will work with licensees to implement them.

by April 29, 2004, for review, revision as appropriate, and approval. The NRC staff is on schedule to complete its review of these plans and will work with licensees to implement them.

The licensees are responsible for providing security for their plants and costs incurred in this process are funded by the licensees. Except for directly after September 11 when Congress specifically authorized money for regulatory costs for upgrading NRC security, almost all of the Federal regulatory costs are paid by the NRC licensees through payment of fees.

Design Basis Threat and New Threat Level

Security programs at NRC-licensed nuclear power plants and certain fuel cycle facilities are designed to protect against an NRC specified level of threat called the design basis threat. The NRC first promulgated its design basis threats (DBTs) for radiological sabotage -- applicable to nuclear power plants -- and theft or diversion of strategic special nuclear material -- applicable to certain fuel cycle facilities -- in the late-1970s. In general terms, DBTs describe the attributes of a hypothetical adversary that these facilities must defend against with high assurance, including numbers of adversaries, types of weapons, and offensive strategies that would be employed by the adversaries. The threat attributes enumerated in the DBTs are based on extensive analyses by the NRC and discussion with the Intelligence Community and law enforcement officials. The DBT received periodic reviews by the staff and Commission resulting in at least one significant upgrade to the DBT prior to the September 11, 2001, attacks. When approved by the Commission, the DBT represents the characteristics of an adversary that a private guard force for a commercial nuclear facility should reasonably be required to protect against.

Following the September 11, 2001, attacks, the NRC conducted a comprehensive review of NRC's safeguards and security programs. This included a reassessment of the DBTs. As a result, the threat characteristics set forth in NRC regulations were supplemented by Orders issued to power reactors and to certain fuel cycle facilities in April 2003.

During its comprehensive review, the NRC staff also participated in the multi-agency working group developing the DOE/DOD Postulated Threat which, although not intended to apply to the commercial nuclear sector, provided insights considered in the development of NRC's supplemented DBTs. Additional coordination was conducted between NRC and DOE to ensure a clear understanding of the differences between the agencies' DBTs. This resulted in a proposed revision to NRC's threat characteristics which were presented to the Commission for their consideration to impose on specific licensees. In January 2003, the NRC sought comments on the supplement to the DBT from State agencies, Federal agencies, and licensees who were authorized access to the information. The Commission considered this information in establishing the supplemental requirements to implement the DBT. In addition, meetings were held with stakeholders, including other Federal agencies, State authorities, and industry representatives. Comments developed during those meetings, as well as the NRC staff final views were provided to the Commission in April 2003.

The Orders of April 29, 2003, required nuclear power plant licensees to revise their security and contingency plans to defend against the supplemented DBT. The NRC is currently reviewing these revised plans for nuclear power plants and certain nuclear fuel facilities, nearly 200 plans in all, and expects that all plans will be reviewed, revised, as appropriate, approved, and, with few exceptions, implemented by the October 29, 2004, deadline imposed by the Commission's April 29, 2003, Orders. As was the case prior to September 11, the Commission

The NRC has been working with DHS, the White House Homeland Security Council, and other agencies regarding an "integrated response" by government assets to help defend against threats that could exceed the DBTs. The concept of "integrated response" applies to both prevention of and response to a potential terrorist event. The NRC is participating in tabletop exercises involving a number of Federal, State, and local agencies at nuclear power plants and continues to support the Homeland Security Council and DHS, the FBI, DoD, and other Federal, State, and local authorities regarding integrated response capabilities.

Vulnerability Assessment and Mitigation Strategies

The NRC has completed an extensive set of vulnerability assessments and identified mitigation strategies for NRC-licensed activities involving radioactive materials and nuclear facilities. Thus far, the results of these studies have validated the actions NRC has taken to enhance security as well as shown areas as needing improvement. These efforts have continued to affirm the robustness of these facilities, the effectiveness of redundant systems and defense-in-depth design principles, and the value of effective programs for operator training and emergency preparedness.

Our vulnerability studies confirm that it would be difficult for even determined adversaries to both damage the reactor core and release radioactivity that could affect public

health and safety. Further, the studies confirm that even in the unlikely event of a radiological release due to terrorist use of a large aircraft, NRC's emergency planning basis remains valid. The aircraft vulnerability studies also indicate that significant damage to a spent fuel pool is not likely, that it is highly unlikely that the impact on a dry spent fuel storage cask would cause a significant release of radioactivity, and that the impact of a large aircraft on a transportation cask would not result in a release of radioactive material. Measures are in place to adequately protect the public from attacks on spent fuel, in either wet or dry configurations. Thus, we conclude that nuclear power plant safety, security, and emergency planning programs continue to provide reasonable assurance of adequate protection of the public health and safety and protection of the common defense and security.

Force-on-Force Exercises

We have continued to improve our security performance evaluation program (our force-on-force evaluations), which we consider an important element for ensuring protection of the Nation's critical infrastructure. In February 2003, we resumed the force-on-force program in the form of a pilot program to test recent program enhancements. In February 2004, the NRC began a transition force-on-force program, incorporating the lessons learned during the pilot program. The transition program follows the same format as the pilot program; however, the "mock adversary" force now uses the characteristics of the Design Basis Threat (DBT), as enhanced and supplemented by our Orders, to prepare for resumption of the full security performance assessment program in November 2004. Under that program, we will conduct approximately 22 force-on-force exercises per year, so that each site's security will undergo an NRC evaluated exercise at least once every three years. This represents a significant increase in the

exercise frequency; in addition, each plant is required to conduct independent exercises at least once each year.

During the pilot program, the NRC identified the need to improve the offensive capabilities, consistency, and effectiveness of the exercise adversary force. The Commission addressed this need by directing the staff to develop a training standard for a Composite Adversary Force (CAF). The CAF for a given NRC-evaluated force-on-force exercise will comprise security officers from various nuclear power facilities (excluding the licensee being evaluated) and will have been trained in offensive, rather than defensive, skills to perform the adversary function.

Baseline Inspection Program

The NRC's oversight program for security is far broader than the force-on-force exercises, vulnerability assessments, strategic and tactical threat assessment, and security plan reviews. It also includes a comprehensive baseline inspection program to verify the continued effectiveness of security measures and confirm compliance. The baseline inspection program for power reactors is part of NRC's Reactor Oversight Program. Through a sampling of licensee security activities, the NRC assesses whether the licensee's security program complies with requirements and provides adequate protection against the DBT for radiological sabotage. Before September 11, the NRC security oversight program focused on four key areas. Shortly after the September 11 attacks, the NRC appropriately refocused portions of its inspection program on verifying licensee implementation of the upgrades specified in NRC-issued advisories and Orders.

Since then, the NRC has substantially revised the baseline inspection program and involved the NRC on-site resident inspectors to a greater degree than before in overseeing security at the plants, ensuring that the NRC has real-time assessments of the status of security on the sites. The NRC implemented a revised baseline inspection program in mid-February 2004 that focuses on an expanded set of key areas, including: (1) access authorization, (2) access controls, (3) security plan changes, (4) contingency response and force-on-force testing, (5) security equipment performance, testing, and maintenance, (6) security training, (7) fitness for duty program, (8) owner controlled area controls, (9) information technology security, (10) material control and accountability, and (11) physical protection of shipments of spent fuel.

The NRC is continuing to enhance and adjust the oversight program for security by developing and implementing more effective processes to assess the significance of inspection findings, more meaningful performance indicators, and revised inspection procedures as a result of the ongoing vulnerability assessment activities and related mitigating strategies.

These changes have allowed the NRC to enhance the effectiveness and efficiency of its oversight of the security measures deemed essential by the Commission after the September 11 attacks. Onsite security inspection hours per year have increased considerably since September 11. Through audits and inspections of the security programs, NRC inspectors confirm that the required security enhancements are implemented.

Status of Security Plan Reviews

As discussed above, in Orders issued on April 29, 2003, the NRC required that licensees take steps to increase protections against a new level of threat, including changes to the adversary force composition and characteristics in light of information gained from the Intelligence Community since September 11, 2001. As part of the Orders, we required nuclear power reactor and certain fuel cycle facilities to develop new security plans, safeguards contingency plans, and training and qualification plans, and to submit them to the NRC by April 29, 2004, for review and approval. The purpose of the Commission's action was to ensure that licensees' plans were revised to specifically describe how the requirements in the NRC's security regulations and post-September 11 Orders were or will be implemented.

When fully implemented, the measures described in the revised plans provide greater capability to respond to more robust attacks than previously required. The new plans also cover a broader spectrum of contingency actions, provide for better trained and qualified security force members, and ensure that more time is devoted to exercises and drills designed to improve the skills of the licensees' guard forces.

The NRC assembled a dedicated team of NRC staff members to review the plans submitted by the industry. As of today, the NRC staff is completing its technical reviews of these plans, and is now working to complete the necessary written safety evaluations and licensing documents to formalize analysis and conclusions associated with each plan review.

Emergency Preparedness

The NRC has long required that its licensees maintain and frequently exercise plans designed to deal with response to emergencies at their plants. State and local agencies, and sometimes Federal agencies, participate in these exercises. The scenarios developed for these plans include many catastrophic events, which are the result of equipment malfunctions, operator errors, or natural disasters. The NRC continues to work with the U.S. Department of Homeland Security and other Federal agencies to integrate Federal Response Plans into a unified National Response Plan and National Incident Management System, and to refine the National Preparedness Policy. We have also completed the development of the commercial Nuclear Reactors, Materials, and Waste Key Resource Plan for Critical Infrastructure Protection. This document serves as the Sector-Specific component of the National Infrastructure Protection Plan. In addition, we continue to coordinate protective strategies with various components of the U.S. Department of Defense, including NORTHCOM and NORAD, and have recently participated in exercises such as Unified Defense '04 and Amalgam Virgo '04. The NRC has revised its Strategic Plan to enhance the recognition of the importance of physical security and emergency preparedness, and licensees will be expected to maintain a high level of preparedness and performance in these areas.

Sharing of Information

The NRC has sought stakeholder input for the many actions taken since September 11. Due to the sensitive, non-public nature of most of the security information, there have been

limitations on public access. In order to expand the sphere of the discussion as far as possible, the NRC has had State outreach meetings, a workshop attended by State and local government homeland security advisors, and public meetings to discuss security. The NRC also posts information on its web site to keep the public informed of actions taken and plans for the future.

In coordination with other Federal agencies, the NRC developed a database of reported security incidents, referred to as the Security Information Database (SID), which contains security reports issued by nuclear plant licensees as a result of advisories that NRC issues. Each report that NRC receives and adds to the SID provides details about a specific security incident that has occurred at a nuclear plant (e.g., suspicious person, suspicious activity, flyovers) and the actions that plant officials are taking to address the incident. SID reports are considered sensitive information and are handled accordingly. This information is posted on a protected web site and shared with authorized nuclear industry officials and Federal, State, and local government agencies.

The NRC is committed to ensuring openness in its regulatory programs and makes every attempt to make as much information as possible available to the public, as well as obtain public input in its decision making. At the same time, the NRC is necessarily interested in ensuring that sensitive information regarding nuclear facilities does not fall into the hands of those who wish to do us harm. After careful consideration, the Commission has decided that certain security information, previously released to the public, will no longer be publicly available and will no longer be updated on our web site. The NRC's public web site will continue to display performance indicators, inspection reports, and other information not related to plant security. The Commission's decision enhances the protection of information related to the

security of licensed facilities, but will not diminish NRC's commitment to openness in carrying out our public health and safety responsibilities.

Addressing the desire of local officials to more frequently and directly communicate with NRC on emergency preparedness, we increased our interactions with State and local emergency preparedness officials. We have supported workshops, meetings and other activities addressing emergency planning issues such as potassium iodide use, radiological dose assessment, communications during event response, and the like. We will continue these efforts whenever important, specific issues are raised.

NRC Computer Security

The NRC recognizes the importance of providing a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provides for development and maintenance of controls required to protect Federal information and information systems. The NRC has historically been focused on technical safety and security issues, and computer security is another facet of that overall concern. Congressional oversight and participation in Federal Chief Information Officer groups have helped focus our computer security efforts to more effectively protect our computer systems. NRC has had a computer security program since 1980 and our focus on computer security from project inception and throughout the project life cycle has enabled us to appropriately protect our computer systems.

The NRC received an "A" on the Federal computer security report card issued by the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. The NRC operates with offices across the Nation and interacts with the public in general informational, regulatory, and discovery interchanges. In each of these interchanges, we take the inherent computer security requirements very seriously and work toward a seamless integration of computer security in our day-to-day operations.

Legislative Needs

Over the years, the NRC has repeatedly expressed its support for enactment of legislation needed to strengthen the security of facilities regulated by the Commission. Although the Commission has used existing authority to ensure robust security for nuclear power plants and high risk radioactive materials, prompt enactment of these provisions would grant the statutory authority for steps that we believe should be taken to further enhance the protection of the country's nuclear infrastructure and prevent malevolent use of radioactive material.

The proposals that the Commission believes to be most important are: (1) authorization of security personnel at NRC-regulated facilities and activities to receive, possess, and, in appropriate circumstances, use more powerful weapons against terrorist attacks, (2) enlargement of the classes of NRC-regulated entities and activities whose employees are subject to fingerprinting and criminal history background checks, (3) Federal criminalization of unauthorized introduction of dangerous weapons into nuclear facilities, (4) Federal

criminalization of sabotage of additional classes of nuclear facilities, fuel, and material, and (5) extension of NRC's regulatory oversight to discrete sources of accelerator-produced radioactive material and radium-226.

All but the last of these provisions are contained in H.R. 6, as approved by the conferees on that bill in the first session of this Congress, and in S. 2095, which has been introduced in this session. The major part of the last provision is contained in S. 1043, which was reported by the Senate Committee on Environment and Public Works in the first session of this Congress. Accelerator-produced radioactive material and radium-226 are not now covered by the Atomic Energy Act, and while there is other radioactive material that is not subject to the regulatory authority of the NRC, discrete sources of accelerator-produced radioactive material and radium-226 are of the greatest concern in our effort to develop uniform national standards to prevent malevolent use of nuclear material.

A copy of the five proposals listed above has been appended to this testimony and the Commission looks forward to working with you on their enactment in this session of Congress.

I appreciate the opportunity to appear before you today and look forward to answering any questions you may have.

Appendix

NRC-REQUESTED NUCLEAR SECURITY LEGISLATION

SEC. 1. FINGERPRINTING FOR CRIMINAL HISTORY RECORD CHECKS.

(a) In General- Subsection a. of section 149 of the Atomic Energy Act of 1954 (42 U.S.C. 2169(a)) is amended--

(1) by striking `a. The Nuclear' and all that follows through `section 147.' and inserting the following:

`a. In General-

`(1) REQUIREMENTS-

`(A) IN GENERAL- The Commission shall require each individual or entity--

`(i) that is licensed or certified to engage in an activity subject to regulation by the Commission;

`(ii) that has filed an application for a license or certificate to engage in an activity subject to regulation by the Commission; or

`(iii) that has notified the Commission, in writing, of an intent to file an application for licensing, certification, permitting, or approval of a product or activity subject to regulation by the Commission,

to fingerprint each individual described in subparagraph (B) before the individual is permitted unescorted access or access, whichever is applicable, as described in subparagraph (B).

`(B) INDIVIDUALS REQUIRED TO BE FINGERPRINTED- The Commission shall require to be fingerprinted each individual who--

`(i) is permitted unescorted access to--

`(I) a utilization facility; or

`(II) radioactive material or other property subject to regulation by the Commission that the Commission determines to be of such significance to the public health and safety or the common defense and security as to warrant fingerprinting and background checks; or

`(ii) is permitted access to safeguards information under section 147.';

(2) by striking `All fingerprints obtained by a licensee or applicant as required in the preceding sentence' and inserting the following:

`(2) SUBMISSION TO THE ATTORNEY GENERAL- All fingerprints obtained by an individual or entity as required in paragraph (1)';

(3) by striking `The costs of any identification and records check conducted pursuant to the preceding sentence shall be paid by the licensee or applicant.' and inserting the following:

`(3) COSTS- The costs of any identification and records check conducted pursuant to paragraph (1) shall be paid by the individual or entity required to conduct the fingerprinting under paragraph (1)(A).'; and

(4) by striking `Notwithstanding any other provision of law, the Attorney General may provide all the results of the search to the Commission, and, in accordance with regulations prescribed under this section, the Commission may provide such results to licensee or applicant submitting such fingerprints.' and inserting the following:

`(4) PROVISION TO INDIVIDUAL OR ENTITY REQUIRED TO CONDUCT FINGERPRINTING- Notwithstanding any other provision of law, the Attorney General may provide all the results of the search to the Commission, and, in accordance with regulations prescribed under this section, the Commission may provide such results to the individual or entity required to conduct the fingerprinting under paragraph (1)(A).'.

(b) Administration- Subsection c. of section 149 of the Atomic Energy Act of 1954 (42 U.S.C. 2169(c)) is amended--

(1) by striking `, subject to public notice and comment, regulations--' and inserting `requirements--'; and

(2) by striking, in paragraph (2)(B), `unescorted access to the facility of a licensee or applicant' and inserting `unescorted access to a utilization facility, radioactive material, or other property described in subsection a.(1)(B)'.

(c) Biometric Methods- Subsection d. of section 149 of the Atomic Energy Act of 1954 (42 U.S.C. 2169(d)) is redesignated as subsection e., and the following is inserted after subsection c.:

`d. Use of Other Biometric Methods- The Commission may satisfy any requirement for a person to conduct fingerprinting under this section using any other biometric method for identification approved for use by the Attorney General, after the Commission has approved the alternative method by rule.'.

SEC.2. USE OF FIREARMS BY SECURITY PERSONNEL OF LICENSEES AND CERTIFICATE HOLDERS OF THE COMMISSION.

Section 161 of the Atomic Energy Act of 1954 (42 U.S.C. 2201) is amended by adding at the end the following subsection:

`(z)(1) notwithstanding section 922(o), (v), and (w) of title 18, United States Code, or any similar provision of any State law or any similar rule or regulation of a State or any political subdivision of a State prohibiting the transfer or possession of a handgun, a rifle or shotgun, a short-barreled shotgun, a short-barreled rifle, a machinegun, a semiautomatic assault weapon, ammunition for the foregoing, or a

large capacity ammunition feeding device, authorize security personnel of licensees and certificate holders of the Commission (including employees of contractors of licensees and certificate holders) to receive, possess, transport, import, and use 1 or more of those weapons, ammunition, or devices, if the Commission determines that--

`(A) such authorization is necessary to the discharge of the security personnel's official duties; and

`(B) the security personnel--

`(i) are not otherwise prohibited from possessing or receiving a firearm under Federal or State laws pertaining to possession of firearms by certain categories of persons;

`(ii) have successfully completed requirements established through guidelines implementing this subsection for training in use of firearms and tactical maneuvers;

`(iii) are engaged in the protection of--

`(I) facilities owned or operated by a Commission licensee or certificate holder that are designated by the Commission; or

`(II) radioactive material or other property owned or possessed by a person that is a licensee or certificate holder of the Commission, or that is being transported to or from a facility owned or operated by such a licensee or certificate holder, and that has been determined by the Commission to be of significance to the common defense and security or public health and safety; and

`(iv) are discharging their official duties.

`(2) Such receipt, possession, transportation, importation, or use shall be subject to--

`(A) chapter 44 of title 18, United States Code, except for section 922(a)(4), (o), (v), and (w);

`(B) chapter 53 of title 26, United States Code, except for section 5844; and

`(C) a background check by the Attorney General, based on fingerprints and including a check of the system established under section 103(b) of the Brady Handgun Violence Prevention Act (18 U.S.C. 922 note) to determine whether the person applying for the authority is prohibited from possessing or receiving a firearm under Federal or State law.

`(3) This subsection shall become effective upon the issuance of guidelines by the Commission, with the approval of the Attorney General, to govern the implementation of this subsection.

`(4) In this subsection, the terms `handgun', `rifle', `shotgun', `firearm', `ammunition', `machinegun', `semiautomatic assault weapon', `large capacity ammunition feeding device', `short-barreled shotgun', and `short-barreled rifle' shall have the meanings given those terms in section 921(a) of title 18, United States Code.'.

SEC.3. UNAUTHORIZED INTRODUCTION OF DANGEROUS WEAPONS.

Section 229 a. of the Atomic Energy Act of 1954 (42 U.S.C. 2278a(a)) is amended in the first sentence by inserting `or subject to the licensing authority of the Commission or to certification by the Commission under this Act or any other Act' before the period at the end.

SEC. 4. SABOTAGE OF NUCLEAR FACILITIES OR FUEL.

(a) In General- Section 236 a. of the Atomic Energy Act of 1954 (42 U.S.C. 2284(a)) is amended--

(1) in paragraph (2), by striking `storage facility' and inserting `storage, treatment, or disposal facility';

(2) in paragraph (3)--

(A) by striking `such a utilization facility' and inserting `a utilization facility licensed under this Act'; and

(B) by striking `or' at the end;

(3) in paragraph (4)--

(A) by striking `facility licensed' and inserting `, uranium conversion, or nuclear fuel fabrication facility licensed or certified'; and

(B) by striking the comma at the end and inserting a semicolon; and

(4) by inserting after paragraph (4) the following:

`(5) any production, utilization, waste storage, waste treatment, waste disposal, uranium enrichment, uranium conversion, or nuclear fuel fabrication facility subject to licensing or certification under this Act during construction of the facility, if the destruction or damage caused or attempted to be caused could adversely affect public health and safety during the operation of the facility;

`(6) any primary facility or backup facility from which a radiological emergency preparedness alert and warning system is activated; or

`(7) any radioactive material or other property subject to regulation by the Nuclear Regulatory Commission that, before the date of the offense, the Nuclear Regulatory Commission determines, by order or regulation published in the Federal Register, is of significance to the public health and safety or to common defense and security,'.

(b) Penalties- Section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284) is amended by striking `$10,000 or imprisoned for not more than 20 years, or both, and, if death results

to any person, shall be imprisoned for any term of years or for life' both places it appears and inserting `$1,000,000 or imprisoned for up to life without parole'.

SEC.5. TREATMENT OF ACCELERATOR-PRODUCED AND OTHER RADIOACTIVE MATERIAL AS BYPRODUCT MATERIAL

(a) DEFINITION OF BYPRODUCT MATERIAL.--Section 11 e. of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (e)) is amended--

(1) by striking "The term 'byproduct material' means" and inserting the following: "The term 'byproduct material' means–";

(2) by inserting on the line following "The term 'byproduct material' means–" the clause in section 11 e. that begins "(1) any radioactive material";

(3) by striking ", and" at the end of clause (1) of section 11 e. and inserting ";";

(4) by inserting on the line following the semicolon added by clause (3) the clause in section 11 e. that begins "(2) the tailings or wastes";

(5) by striking "content." at the end of clause (3) in section 11 e. and inserting "content; and"; and

(6) by inserting on the line following "content; and" the following:

"(3)(A) any discrete source of radium-226 that is produced, extracted, or converted after extraction, before, on, or after the date of enactment of this paragraph, for use in a commercial, medical, or research activity; or

"(B) any material that --

"(i) has been made radioactive by use of a particle accelerator; and

"(ii) is produced, extracted, or converted after extraction, before, on, or after the date of enactment of this paragraph, for use in a commercial, medical, or research activity; and

"(4) any discrete source of naturally occurring radioactive material, other than source material that --

"(A) the Nuclear Regulatory Commission determines (after consultation with the Administrator of the Environmental Protection Agency, the Secretary of Energy, the Secretary of Homeland Security, and the head of any other appropriate Federal agency), would pose a threat similar to that posed by a discrete source of radium-226 to the public health and safety or the common defense and security; and

"(B) before, on, or after the date of enactment of this paragraph, is extracted or converted after extraction, for use in a commercial, medical, or research activity.".

(b) AGREEMENTS.--Section 274 b. of the Atomic Energy Act of 1954 (42 U.S.C. 2021) is amended--

(1) by redesignating paragraphs (3) and (4) as paragraphs (5) and (6), respectively; and

(2) by inserting after paragraph (2) the following:

"(3) byproduct materials (as defined in section 11 e.(3));

"(4) byproduct materials (as defined in section 11 e.(4));".

(c) REGULATIONS.--

(1) IN GENERAL.--Not later than the effective date of this section, the Nuclear Regulatory Commission shall promulgate final regulations establishing such requirements and standards as the Commission considers necessary for the acquisition, possession, transfer, use, or disposal of byproduct material (as defined in paragraphs (3) and (4) of section 11 e. of The Atomic Energy Act of 1954 (as added by subsection (a))).

(2) COOPERATION.--The Commission shall cooperate with the States in formulating the regulations under paragraph (1).

(3) TRANSITION.--To ensure an orderly transition of regulatory authority with respect to byproduct material as defined in paragraphs (3) and (4) of section 11 e. of the Atomic Energy Act of 1954 (as added by subsection (a)), not later than 180 days before the effective date of this section, the Nuclear Regulatory Commission shall prepare and provide public notice of a transition plan developed in coordination with States that--

(A) have not, before the effective date of this section, entered into an agreement with the Commission under section 274 b. of the Atomic Energy Act of 1954 (42 U.S.C. 2021); or

(B) in the case of a State that has entered into such an agreement, has not, before the effective date of this section, applied for an amendment to the agreement that would permit assumption by the State of regulatory responsibility for such byproduct material.

(d) WASTE DISPOSAL.--

(1) Notwithstanding any other Federal or State law or any action that has been taken to implement such law, commencing with the effective date of subsection (a), byproduct material as defined in section 11 e.(3) and (4) of the Atomic Energy Act of 1954 may be transferred to and disposed of--

(A) in a disposal facility licensed by the Commission, if the disposal meets the requirements of the Commission, or

(B) in a disposal facility licensed by a State that has entered into an agreement with the Commission under section 274b. of the Atomic Energy Act of 1954, if the disposal meets requirements of the State that are equivalent to the requirements of the Commission.

(2) Notwithstanding the provisions of paragraph (1), byproduct material as defined in section 11 e.(3) and (4) of the Atomic Energy Act of 1954 may be disposed of under the provisions of Title II of the Solid Waste Disposal Act (42 U.S.C. 6901 et seq.), popularly known as the "Resource Conservation and Recovery Act," to the same extent as such material was subject to those provisions before the enactment of this section.

(3) Byproduct material as defined in section 11 e.(3) and (4) of the Atomic Energy Act of 1954 shall not be considered low-level radioactive waste as defined in title I of the Low-Level Radioactive Waste Policy Amendments Act of 1985, or in

implementing any Congressionally approved Compact entered into pursuant to the Low-Level Radioactive Policy Act of 1980 as amended.

(e) EFFECTIVE DATE.--Except with respect to matters that the Nuclear Regulatory Commission determines are required to be addressed earlier to protect the public health and safety or to promote the common defense and security, the amendments made by this section take effect on the date that is 4 years after the date of enactment of this Act.

Mr. SHAYS. You may go to the next witness.

Mr. TURNER [presiding]. I'm sorry.

Mr. Zimmerman.

Mr. ZIMMERMAN. I have no opening statement. Thank you.

Mr. TURNER. We will go to a 5-minute round of questions from the members of the committee.

I know many of the members of the committee are going to have questions concerning the design basis threat, their concern of its insufficiency. The concern of force-on-force exercises and their lack of reliable training and effectiveness, also issues concerning equipment and training.

But I am very interested in the relationship between DOD and the protection of our nuclear power plants. In some of the information that we have indicates that power plants are not required as part of their design basis threat to take into consideration attacks by a foreign power or even perhaps the type of terrorist organizations that we see with al Qaeda, with the airborne threat.

Could you talk a little bit about the NRC's coordination with the DOD and how and where that occurs? Both in the level of communication, exercises, onsite equipment and response?

Mr. REYES. OK. Prior to September 11th, the NRC has always had intelligence analysts. Subsequent to September 11th those intelligence analysts—even though they are NRC employees—are collocated with the intelligence agencies. So we have changed not only the analysis of intelligence information the way we did it before, but now we have collocated with the intelligence community. And what that has provided is a more direct feedback for us—but we now provide the intelligence community, information we didn't provide it before. We have required our licensees to report to us activities that may observe around their facilities that may have some bearing on the national intelligence information.

Now, in terms of the design basis threat, we have worked very closely with DOE and DOD in terms of the intelligence to determine our design basis threat. As somebody stated, we do not have in the NRC regulatory oversight weapons plans that have nuclear weapons or plants that have nuclear weapons components. So our design basis threat takes that into account and we feel is similar to DOE facilities that are similar to ours. So we think that the design basis threat is similar now.

Now, I couldn't bring all of the pictures because security information. It's limited to the public. But some of the pictures here provide some of the features that the plants have. They compare to similar facilities with DOE and DOD. What you don't see here today is technology to detect intrusion and some of the programs that they have the facilities to make sure that the individuals that have access to the facility have security clearance——

Mr. TURNER. I am going to interrupt you. Because we have a limited time period for the answers. I appreciate your giving us information concerning intelligence gathering and information with respect to detection.

Mr. REYES. OK.

Mr. TURNER. But obviously my question and my interest concerns the ability to actually defend these facilities. Intelligence is only an element that gives you an understanding of what you are

defending against or when defense is necessary. And detection certainly is way too late. So if you could please describe with respect to the Department of Defense, NORTHCOM, where are you drawing the line between the facilities responsibilities, the DOD's responsibilities and how are those actually being coordinated in a meaningful way that actually transcends into defense.

Mr. REYES. Let me have Mr. Zimmerman give you the details of our interface with NORTHCOM.

Mr. ZIMMERMAN. Thank you let me provide you with some of the specifics. With regard to NORAD, we have interactions with NORAD on a daily basis. We provide them information associated with the status of our facilities. They know which facilities are operating, which ones are shut down, which facilities may be with selected equipment out of service. We have run exercises with NORAD, where we have Amalgam Virgo or Amalgam Amigo are examples, for example, of actual interactions we have had with them on the phone, as well as with licensees.

There is also, have been calls that NORAD has had directly with our licensees, but we have set up a protocol that happens very quickly. If there's an anomalous situation in the air that involves NORAD, NRC and the licensee on a three-way phone call—and we have been practicing that with our licensees—we have been involved in many exercises with the Federal Government and DOD primarily in the lead. We have been involved with the TOPOFF exercises that have occurred. We are involved with TOPOFF planning for next year. We have been involved in Forward Challenge, we have been involved with UDO 4.

We are actively involved in and are interacting both with NORTHCOM with regard to their ability to respond with quick response forces. They have been out to the sites. We have taken them onsite tours. And they have had an opportunity to walk the facilities share their thoughts with us.

So we view that we have a very strong relationship with NORAD, with NORTHCOM and we plan on making it stronger through an effort we call integrated response planning. And that deals with recognizing that the design basis threat we view as what is reasonable for private guard force, where the Federal Government needs to come in promptly. DOD is an active player in that effort of integrated response.

Mr. TURNER. Mr. Kucinich.

Mr. KUCINICH. Thank you very much, Mr. Turner.

Mr. Zimmerman, one of the things the NRC points to on their Web page is a way that increased security is extending the perimeter of their facilities. Despite this, there have been two incursions into nuclear facilities in the last 2 months. One occurred at Beaver Valley in Pennsylvania and the other occurred at Pilgrim. If NRC had indeed extended the perimeter, ostensibly to catch terrorists before they get on the site, how were these individuals able to get out into plant sites?

Mr. ZIMMERMAN. I think context is very important in this regard. Without talking to the specific details—I am not sure I recall the specific details—the area that we are talking about at these facilities is what is called the owner-controlled area. This is the area of property that is owned by the licensee, but in many cases is far re-

moved from where the protected area where the vital equipment is located. At some plants, it's miles away from where the actual facility equipment is located. What we have done subsequent to September 11 is require that licensees conduct surveillance out in their owner-controlled area to be able to identify the possibility of surveillance taking place on their site or as well as any plant, preplanning for an attack.

We also called for licensees to mix up those patrols so they don't always roll around at 4, you know, hour on the hour. They mix it up to try to keep any potential surveillance, you know, at bay. We get daily reports that are made from the licensees into my office that address the many instances where individual sightseers are taking pictures of the sites, where the film is confiscated, explain to the individuals the sensitive nature of the equipment that they are trying to take pictures of.

There are close working relationships with the local law enforcement and the FBI to run license plates to look for any information in the background of these individuals. It's a very aggressive program—and addressing one of the other concerns that was raised earlier, we share this information across the industry so that if there is some information that somebody sped away quickly from a particular location, that information is put on a protected Web server so all sites have access to it and can be on the lookout for a similar vehicle.

Mr. KUCINICH. I have a number of questions here, Mr. Chairman, that will probably require—you are going to have a second round of questioning? I know my time isn't up.

Mr. SHAYS [presiding]. I would be happy to yield to my colleague some of my time. We would like to go just a 5-minute round with this, and then they are going to come back after GAO has testified.

Mr. KUCINICH. Well, before——

Mr. SHAYS. Why don't we go through this. Why don't we——

Mr. KUCINICH. My 5 minutes hasn't expired.

Mr. SHAYS. OK.

Mr. KUCINICH. I want to, as a personal matter ask you a question.

Mr. ZIMMERMAN. Surely.

Mr. KUCINICH. What do you think about the failure of your own agency to provide information to the public about a hole in the head of a reactor vessel. Is that a security matter that you have any concern with, or is that somebody else's job?

Mr. ZIMMERMAN. To be candid, it is not in the realm of responsibilities that I have. I think better justice could be done to answering your questions in a different setting, perhaps with different individuals that are closer.

Mr. KUCINICH. You really don't know anything about that, is that what you are saying?

Mr. ZIMMERMAN. No, I am not saying that at all.

Mr. KUCINICH. Do you know anything about it at all?

Mr. ZIMMERMAN. Yes.

Mr. KUCINICH. What are you aware about it?

Mr. ZIMMERMAN. I am aware of the fact that there was degradation in the vessel head that was late in being identified, through a non-destructive examination. I am aware of the fact that the

NRC followed the degradation closely and had identified a period of time that it was felt that it was reasonable for that facility to continue to operate based on the information that was available to them.

Mr. KUCINICH. Mr. Chairman, I just want to point something out. And I don't think this is tangential. We have a witness in front of us whose job deals with nuclear security. I would submit that there is a lack of communication within the NRC on issues of security that he just made a statement that defies belief of anyone who claims that they followed this. So I am just going to take his initial statement that he is really not responsible for this. And the gentleman is showing a lack of comprehensive understanding of what the NRC's failings were on this—and I am not going to attribute that to his problem—I am going to attribute it to the responsibilities of the people who had the first obligation to let the public know—should have also let him know, since he is dealing with nuclear security.

So I think one of the things the committee has already been able to determine here is that you don't have the kind of communication within the NRC that would protect the public interest with respect to security lapses of a mechanical kind, physical kind, inside. So the security problems can come outside, but they can also come inside.

Thank you, Mr. Chairman.

Mr. TURNER [presiding]. Mrs. Maloney.

Mrs. MALONEY. What have you done to protect our plants from the possibility of a plane flying in?

Mr. REYES. Yes, we have——

Mrs. MALONEY. We have read in the 9/11 Commission said that was one of their plots. So how are we protecting ourselves from that?

Mr. REYES. The NRC has done a vulnerability assessment. That includes a wide variety of aircraft. It includes smaller aircraft, all the way to a large commercial aircraft loaded with fuel—an analysis of a limited number of plants that are typical in the design of the power plants in the United States. What that analysis has shown is there is a very low probability that the crash of such a large aircraft into the facility would cause both damage to the core and a significant radiation release that will impact the health of the public.

And the reason being is that prior to September 11th, these plants have severe accident procedures—they were procedures that were mitigated or strategies that were to cope with events that could not be foreseen by the design. Our analysis has identified that more had to be done—and in fact the mitigative strategies have been enhanced to cope with such an attack. Now that will be the back end once the attack occurs.

At the front end, I think Mr. Zimmerman talked about our relationship with NORTHCOM and NORAD and the exercises and direct communication from NORAD to the control room in the power plant to advise them if there is a pending attack.

Mrs. MALONEY. Do we have any planes in the air that would shoot down another plane coming? I mean, we never anticipated that a plane would knock down the Towers. So the main thing is

to prevent it from coming in in the first place. So what do we have? Are you working with the—you understand the security to basically shoot down a plane if it ever got into the area?

Mr. REYES. Yes, our work has been with NORAD who had the responsibility to intercede the aircraft.

Mrs. MALONEY. Now, in the prepared testimony of the GAO, they say that the NRC does not plan to make improvement to the inspection program that the GAO previously recommended and still believes that it is not necessary. For example NRC is not following up to verify that all the violations of security requirements have been corrected. Can you explain that? That's a direct quote from the GAO report that they are very disturbed that you are not correcting the items that they pointed out to you. Why not?

Mr. REYES. The GAO report relates to our followup of the corrective action—the NRC both on the safety and security site. And we don't think distinguish them—they work together—puts their effort on the violations of biggest or higher significance. Now, what we do is we put—confirm all the corrective actions for violations of higher level, and for low level violations we do it in a sample basis. Now that doesn't mean we don't know what was done.

What it means is for security specialists to confirm whether that minor violation or violation of low risk was not corrected. But we have an NRC office in every power plant. We have inspectors there, and we are aware of the corrective action on small, low-risk violations. But we follow all significant violations with subject matter experts, whether security or safety.

On the lower level, we do a sampling process. It's a matter of resources.

Mrs. MALONEY. So, then, you are not following up to verify that the violations of security requirements have been corrected for "smaller violations?"

Mr. REYES. On a sampling basis we do.

Mrs. MALONEY. But you are just correcting the larger violations. Can you give me an example of a smaller violation that you are not correcting?

Mr. REYES. Well, they corrected it. We just don't confirm specifically that it is corrected. I will have Mr. Zimmerman maybe give an example of a minor violation.

Mr. ZIMMERMAN. A minor violation could be an isolated case where an individual had a lapse and didn't record information within a certain period on a tour or potentially may not have logged it at all. We would view that as a violation. By understanding a licensee's program, they have a corrective action program that they are required to have. Their quality assurance organization will pursue that, determine whether it is an isolated case.

We also during our review—if we see something that indicates it is potentially larger and has programmatic aspects to it—we would continue to follow that trail. But if we see that as an isolated case, the corrective action would be taken by the licensee. And then as Mr. Reyes said, we do come back for the lower significance items and do a sampling check to see if we have confidence in the thoroughness of the review of the utility.

Mrs. MALONEY. My time is up. Thank you.

Mr. TURNER. Mr. Platts.

Mr. PLATTS. Thank you, Mr. Chairman. I appreciate your testimony here today. And I question our focus, I know, is about protecting our facilities from the terrorist threats. And I would like to at least put on your radar an issue that kind of relates that if there is an attack and our response and attentions come to my attention in my local community, I would go right up against the Susquehanna River where Three Mile Island is—and certainly as a high school student, remember 1979 very well—living a few miles from the plant.

The issue that has been raised to me is if there would be an attack how we would respond to the attack, specifically for children in day care, preschools, nursery schools, and believed by some of my constituents that NRC's oversight, along with FEMA, is not insuring that our NRC regulations are being fully complied by facilities regarding those preschool child care centers, and the State plans that are in place. My understanding of NRC is your responsibility is really to improve the State plans for evacuation if there is an attack or if there is an incident of whatever kind that requires an evacuation that NRC looks to the State and approves the State plans?

Mr. REYES. FEMA, the Federal Emergency Management Agency does that.

But if I could address briefly your concern. If there is an attack at a nuclear power plant—regardless of whether it is ground, waterborne or air—right away, there is a declaration of high level emergency. What that does is automatically gives the local government, the counties and the State, mobilizing their emergency plan.

And the typical arrangement—and I don't know the one in Pennsylvania specifically—the typical arrangement is that when that is declared, the local government already has prearranged decision-making on evacuating children, senior citizens. So the fact that the facility was attacked without any consequences—yet in terms of release of radiation and all of that—because you declare a high level emergency, you are already as a precautionary measure, very conservative, rolling and the offsite government agencies are already moving.

Mr. PLATTS. The concern is that—and then that process, for it to work, those plants need to be thorough and that the FEMA reviews the plans.

Mr. REYES. Right.

Mr. PLATTS. Based on their finding and you issue a license that yes they have a plan in place.

Mr. REYES. Correct.

Mr. PLATTS. Is that perhaps with some facilities in Pennsylvania and perhaps elsewhere around the country that those plans are not as thoroughly guarding these preschool age children even though the regs require them to, to accomplish those children as well.

Mr. REYES. Yes, it is FEMA that has to do the assessment. And they monitor the exercises and the plant and the fact that it gets performed adequately. I just couldn't——

Mr. PLATTS. So NRC basically takes the decision of FEMA and just ratifies that decision that FEMA says, yes, they are in compliance, their State plan, their local plan, therefore the license is issued?

Mr. REYES. Yes, it's called reasonable assurance. FEMA sends out a report, and a certification that they have reasonable assurance that the offsite emergency preparedness actions, the plans and the actions that they will take by observing the execution of the plan and the exercises, etc. is adequate. And we take that certification of reasonable assurance and accept it.

Mr. PLATTS. Thank you. Thank you, Mr. Chairman.

Mr. TURNER. Ms. Watson.

Ms. WATSON. According to the GAO, NRC is not taking advantage of opportunities to improve the effectiveness of force-on-force exercises and security oversight in general by implementing the recommendations.

And I did hear you mention, you have gone so far with a lack of resources. I would like to elaborate on that and tell us how is nuclear power plant inspection information shared with the NRC regional offices and nuclear power plants. So you can answer collectively.

The other concern that I have is that several months ago, we heard about traditional procedures and traditional ways of calculating how an attack would take place on our nuclear plants. I had problems with traditional. Because I think whatever enemy out there we are facing is being very creative. And if we have a traditional procedure or formula that we use on the ground, what about that comes from the air or over water? So you might want to address that as well.

Mr. REYES. OK. I would be glad to do that. Let me talk first about the information sharing. All the findings, all the violations, whether they are high or low or of significance, regarding security, are reviewed by a panel which is composed of a representative from all of our four regional offices and our headquarters offices.

And that's to make sure that in fact they are properly being categorized in terms of their significance and therefore which ones we need to do followup corrective action in detail and which ones we do a sampling process. That information is shared because there's representatives from each one of the regional office and the program office. So those individuals share that within their own group.

Then we also have very frequent meetings with the industry—it's called a security working group—where we share all the issues that we have identified with them, and the security working group from the industry then shares that with their counterparts.

We also have prepared a protected Web page that has those kindS of information. Not only do we share that with the licensees, but it gets shared with local governments and other interested parties that do have the appropriate clearance to have that information. So we do have a very aggressive way to share the information.

Now, we haven't adopted every recommendation that GAO has submitted. We haven't dismissed them; we are considering them, but we feel there is a very aggressive way that this information is being shared.

Ms. WATSON. When you said lack of resources, would you elaborate, please?

Mr. REYES. We feel we have adequate resources, but what you want to do is you want to put your resources where the more sig-

nificance is. So Mr. Zimmerman provided you an example of where a patrol officer had an oversight to log in as they conducted the patrol around the facility, and they have to log in exactly where they were and where they are not going. That would be a relatively low violation of our requirements, and we necessarily wouldn't put the resources there. If we were to find a more significant problem regarding training of the officers or the weapons not being in good working order or something like that, we will put very detailed followup on the more significance, because they do have the more significant potential to affect security. So there's a matter of grading where our resources go to; they go to the most significant findings.

Ms. WATSON. I am really troubled by the fact that we are fighting an enemy of unknown proportion. It could be an American—I will always remember Oklahoma—or it could be someone who has merged into our society. They have a very different mindset than we do. And I'm wondering if there is any activity going on that tries to get into that mindset, because I think the September 11 attack was planned a decade in advance. And certainly we know by the training, the time it took to train those who flew the planes—and they went in and said we don't want to learn how to take off or land; that should have rung a bell. And they paid in cash. But apparently they were more interested in getting that money than in picking up the clues. And I am finding out there have been clues along the way and we haven't done a good job in connecting the dots.

So I am wondering if we have a think tank that might be looking at the creative ways that people, you know, watching us in an open society might do us great harm through our nuclear plants. Pand, finally, how does this fit into homeland security? How does the NRC, what role do you play in terms of homeland security?

Mr. REYES. OK. Let me talk about—the concerns you had about the potential adversaries and the modes and the planning all goes into the intelligence community. What we do is we take that information, and, for example, when we consider the design basis threat and when we do our exercises, we assume that all that information in terms of what we call coordinated attacks—and we assume they are coming from the ground, from the air, from the water, and that they have an insider that they have. So all that is considered in both the design basis threat and the exercises we actually conduct. So also, we don't go out there to try to do intelligence work. We are the beneficiaries. And by having our intelligence analyst physically present in that community, we get that information and we factor that into our activities.

Now, let me have Mr. Zimmerman explain to you how we work with DHS, because we are an active participant in that effort.

Mr. ZIMMERMAN. One of the things that we do with the Department of Homeland Security is we try to maximize our time that we spend in their operation. And I will explain that. There may not be a particular issue that is necessarily in our sector, but we will try to send people to their operations center, even if there is an issue that they are pursuing that is unrelated to the nuclear sector, just so that we can get comfortable, get a chance to meet people, understand what their protocols are. And we basically have a relatively large number of people that we are sending down there and

getting badged ahead of time, so that if the bell does ring in our sector, we have working relationships established. And if we are in a reactive situation, we know where our desk is, we know what our responsibilities are.

And when we do our exercises now, we have requested of DHS, and they have been very supportive, to try a continuous improvement to make our exercises more realistic, where we want them to play in our exercises now that they have been stood up. So we want to send people to them, understand what issues they would have in this emergency situation during this drill, and raise those issues directly to us in real time in the exercises so that we can practice and learn how we can improve our overall response to the Federal Government.

Ms. WATSON. I will just finish up with this. I think intelligence has failed to provide all of us with the information that we need to prevent—not respond to an emergency, to prevent. And I would hope that the NRC would definitely be looking at strategies, procedures, to prevent a nuclear kind of emergency, because once there is a nuclear attack we are done.

Mr. ZIMMERMAN. May I respond?

Mr. TURNER. Actually, we need to move on. Mr. Tierney.

Mr. TIERNEY. Thank you, Mr. Chairman.

You rely on private companies for the securities of the individual plants. Right?

Mr. ZIMMERMAN. That's correct.

Mr. TIERNEY. All right. So we have 65 plant sites, 103 nuclear reactors in 31 States.

Mr. ZIMMERMAN. Correct.

Mr. TIERNEY. And you sort of delegate that responsibility to private companies, and then rely on their report to you as to whether or not they are complying with the various standards that you set.

Mr. REYES. No. We have direct observation of their activities.

Mr. TIERNEY. About once every 3 years, right?

Mr. REYES. No, no. That's incorrect.

Mr. TIERNEY. OK.

Mr. REYES. See, the inspection program—and I think this is—the GAO auditors are in the process of doing that effort, and they haven't been able to visit the facilities. So we have a security inspection program that looks at everything, from training to performance of the detection system, implementation of the program for access to individuals, communications. The portion as far as exercise is on top of all that I just told you, and that is the final task on the dynamics. That's where we actually simulate adversaries, and they actually come in and jump over the fence and actually have access to—and we simulate the attack. But that's only the culmination of a large number of inspection hours by a lot of subject matter experts in security that come in unannounced at all times of the day or night to check each one of the elements.

Mr. TIERNEY. Let me interrupt if we can because are limited in time here. So you are saying that your agency determines the standards for training, and then you go down and you observe and make sure that training is in fact occurring and being met and that people are passing those criteria.

Mr. REYES. That's correct.

Mr. TIERNEY. And that's no matter what the turnover there.

Mr. REYES. Correct.

Mr. TIERNEY. And then you are telling me that you are also keeping an eye on how much overtime is involved, how many hours these people are working on each shift on a regular basis?

Mr. REYES. We have requirements for that. We review the records and we interview individuals.

Mr. TIERNEY. Did you want to add something?

Mr. REYES. What he was going to tell you is our inspection program has increased by a factor of five.

Mr. ZIMMERMAN. Since 2000. The amount of hours that we spend onsite—this is separate from force on force—is we have gone up fivefold in the amount of inspection hours that we are currently spending onsite. The design basis threat that we issued in April 2003 is quite similar to the interim compensatory measures that we put in place in February 2002. Our inspectors have already gone out and verified that probably 80 percent of what is in the revised 2002 DBT is already in place.

Mr. TIERNEY. Are you subcontracting any of this evaluation work?

Mr. REYES. No.

Mr. ZIMMERMAN. It's being done through our regional offices.

Mr. TIERNEY. And when you do the force on force, are you subcontracting any of that attack force work out?

Mr. REYES. No. The NRC reviews the training for the adversaries, the NRC decides on the scenario, and the NRC is there in large numbers to observe the force on force. And we are the ones who determine whether the performance is acceptable or not. See, this is a big difference between DOE and NRC. DOE operates and regulates itself. We have a private licensee, but we are the ones who do the oversight and we are the ones who determine the adequacy.

Mr. TIERNEY. But it is not your personnel that are actually doing the force on force. You hire somebody to do that, then oversee them?

Mr. REYES. The adversaries are not NRC employees. The people monitoring them and doing the independent assessment are.

Mr. ZIMMERMAN. We hire contractors that are experts in this area. They are joined at the hip with the adversary team; they are in the field with the adversary team as they are trying to make their approach on the facility. They are involved in the preparation aspect indicating, based on what we have been able to determine, this is how I would attack the facility, so this is how you will attack.

The decision on how the attack is made is made by the NRC contractor, not by the contractor that's going to carry out the actual attack. But our contractors will go with them.

Mr. TIERNEY. So we no longer have Wackenhut watching Wackenhut.

Mr. REYES. It never has been. We don't know the misunderstanding, but it never has been.

Mr. ZIMMERMAN. We do the full assessment. Wackenhut will pull the trigger, but we will have somebody there to make sure that person is taking the appropriate action of what he or she has been

instructed to do based on us laying out what the scenario will be, and then being with them in the field while they carry it out.

Mr. TIERNEY. We can maybe revisit that again later. Tell me, if you would, about spent fuel storage security and why we should feel comfortable with the way things are going there.

Mr. REYES. There is two kinds of storage of spent fuel. One is what we call the pools or the wet pool. And those are inside all the protected area of the facility, and all the security features that you have for the reactor, you basically have for the wet pools. The dry cast storage could be either inside the protected area or could be sitting by itself within a protected area. And that also has security features to it. The dry cast storage is more robust in terms of attacks and all that. So we feel very secure that it is—the security is adequate.

Mr. TIERNEY. Thank you.

Mr. TURNER. Mr. Sanders.

Mr. SANDERS. Thank you very much, Mr. Chairman.

As you know, gentlemen—and thank you very much for being with us. As you know, we have a nuclear power plant in Vernon, right at the southern edge of Vermont and right near the Massachusetts border. Recently there was a scare, as you know, when two spent fuel rods appeared to be missing, and they were relocated sometime later. But that raised anxiety in an area where anxiety is already fairly high.

Let me just ask you just a couple of questions. It seems to me—and I don't want to disappoint any of my colleagues or you—that the truth of the matter is there is not an enormous amount of faith in the U.S. Government; that people do not believe everything that you say or I say or anyone else says. And when it comes to nuclear power and the potential danger, clearly people are very, very concerned as to whether or not the U.S. Government is in fact protecting them.

As I understand it, earlier in August the NRC announced that a substantial amount of site-specific security information would be taken off of its Web site. Now, I can understand that we do not want to tell al Qaeda all of the methods that we have to defend nuclear power plants. But the bottom line is that when people, at least in the past, could critique, could say it is not enough, now they have virtually nothing. So if I'm living in Vernon, Vermont or Brodova, Vermont, how do I know that the kind of security—I don't need to know every detail, people understand that. But what kind of reassurance do people have that security is appropriate when they now go to the Web site and they get far less information than they used to? And as I understand it, you took that information off kind of privately, without a lot of public discussion as to whether that was a good idea.

Mr. REYES. Prior to September 11th and today, our strategic plan has safety security and openness as one of the goals. And we have learned since September 11th, through our feedback with the intelligence community, that there are people out there that want to do us harm. And information that we openly share with everybody as one of our strategic goals could be harm to the Nation. So what we had to do is, we had to do some soul-searching and find out what

information should we pull out of the public. And we took out information that could assist somebody in doing us harm.

What we are going to do is—the remaining of the information regarding the safety of the facility, all that information is still there. What we are going to do is we are going to summarize that security information we have and present it in a summary fashion without giving details that somebody can harm us.

Mr. SANDERS. We don't have a lot of time. And I think everybody understands that we do not want to give enemies information. But on the other hand, I would ask you to keep in mind, given the fact that people do not necessarily have a lot of confidence, that they do want to know that they are being protected. They want the opportunity to critique when they feel that security is not appropriate. And I fear very much that is not the situation.

Now, I understand that there was several FOIA requests made before this policy went into effect; in other words, regarding the nature of security. What does the NRC plan to do with those FOIA requests?

Mr. REYES. Well, we are going to have to process them under the new guidelines, because regardless of how you put the information in the public, the details, we now know our intelligence colleagues are telling us do not put detailed information out that can assist people to do us harm.

Mr. SANDERS. Let me go to another area. And forgive me, we just have to move fast because there's not a lot of time. I'm picking up at a point that Mr. Tierney raised a moment ago; and that is, NRC, as I understand it, has repeatedly stated that they believe release of radioactive fuel as a result of a terrorist attack on a spent fuel pool is unlikely. NRC officials have made that point over and over again, and they said that as recently as last week.

So what I want to know is why you think that way? Are you taking additional steps to fortify the many spent fuel pools around the country, rather than simply dismissing the prospect of a breach of security there?

Mr. REYES. We have done analysis of airplane crashes into the spent fuel pools. Now, it's been a limited number of details in terms of which ones we have done that, and those are the conclusions you stated. We are now moving forward to doing further studies to make sure that we have done a thorough review in any one of the layouts. The configuration of the pools are different in different plants, and so we are now continuing the analysis to make sure that the results we have are representative of the total population.

Mr. SANDERS. Am I correct in remembering, though, that there are some knowledgeable people who disagree with some of the conclusions that you have reached about the safety of those facilities in terms of a plane attack?

Mr. REYES. There's always people who disagree.

Mr. SANDERS. I'm not talking about fringy people; but I'm talking about intelligent people.

Mr. REYES. Yeah, there's always intelligent people that disagree with us.

Mr. SANDERS. All right. What about the potential of an air attack? I understand that there is no longer a no-fly zone in effect

over our Nation's nuclear reactors. And my question is, why you think that is good policy? And why does the NRC think it's such an insubstantial threat, especially in light of the fact that al Qaeda clearly considered nuclear reactors an attractive target?

Mr. REYES. After September 11th, we met with the FAA and we tried to get their insights and their determination on what should be the airspace around nuclear power plants determined to be. The FAA determination was that for nuclear power plants and other critical infrastructure, that it was not advisable in their mind to put no-fly zones. What they did determine was for nuclear power plants to put what they call a notice to airmen, which basically is a notice that goes to all pilots about limiting their flying around these facilities. But we are just following, after the meeting with the FAA, what they determined to be the most wise.

Mr. SANDERS. But do you think that makes sense? On the surface it doesn't make a lot of sense to me, given what we saw about September 11 and the use of airplanes as missiles.

Mr. REYES. The rationale of the FAA was that there's other critical infrastructure, just like nuclear power plants. And if they were to put no-fly zones over all these facilities and the infrastructure, you basically stop commerce because you have so many no-fly zones across the national—chemical plants, pesticides.

Mr. SANDERS. Frankly, a nuclear power plant is different than many other infrastructures and facilities. We don't think we should have universal no-fly zones, but I would suggest that maybe we may want to do a little bit of thinking about that one.

Mr. REYES. And we met with the FAA and we tried to convey that.

Mr. SANDERS. I mean, you met with the FAA. You are the experts on nuclear dangers; they are not. They have other interests as well. And we need to rely on somebody to protect us.

Mr. TURNER. Mr. Sanders, we need to move on.

Mr. SANDERS. Thank you.

Mr. TURNER. Chairman Shays.

Mr. SHAYS. I thank you. We are going to have a second opportunity to question these witnesses. We do thank them, because that's a better way for them to make their arguments and for us to understand the challenges.

The bottom line, it's been 3 years since September 11th, and 2 years of it was the intelligence community giving us a postulated threat. You have worked the last year on a design basis threat, and now that's coming into place. And what's concerning me is there appears to be 3 years before you really test at every facility, and so it's going to be like 6 years from September 11th.

I want to ask, are you aware of the memo, which was classified, from the Deputy Secretary of Energy to DOE facilities strengthening the DBT and ordering safeguards beyond those called for by the initial post-September 11 standard?

Mr. REYES. We work closely with DOE, and we know exactly what their DBT is and where the directions are heading. We are required by the Commission to brief them every 6 months on the intelligence, and so they can reassess the DBT. We are scheduled to do that November 16th of this year. At that time, we will brief them not only with the intelligence information we have, but with

all the DOE—DBT changes that they are considering or perhaps they have implemented by the time we meet with the Commission.

Mr. SHAYS. When we met with DOE officials and we toured certain facilities, they came back to us and said that they were going to strengthen their design basis threat. We have the postulated threat up here, we have the Department of Energy with their DBT here, and we see you lower down on the design basis threat, that you don't have as strong a standard as what we see happening for the DOE facilities. That's my reading of it. And I would like to know, do you anticipate strengthening your design basis threat based on——

Mr. REYES. We will share that information with the Commission. It's a policy decision by the commissioners whether to increase or not increase the DBT. And, but we have a process to do that, and November 16th is our next presentation to the Commission to consider that.

Mr. SHAYS. One of the biggest criticisms that GAO has is that they say the NRC's review of the plants, which are not available to the general public for security reasons, has primarily been a paper review and is not detailed enough for NRC to determine if the plans would protect the facility against the threat presented in the DBT. How do you respond to that?

Mr. REYES. The security plans are—they have, but at a pretty high level. And what you see here, what you have at the station, then, is what we call implementing procedures, the strategies of how those individuals will respond to an attack, where are they located, how will the firing lines, etc., is an implementing procedure. And the reason you want to have it that way is, let's assume that the legislative proposal that we highlighted to you gets approved and we now can give them better weapons. Then the strategy at the time may change.

Mr. SHAYS. Well, now that we don't have the assault weapon ban, are you now able to get—no, I'm serious. Are you prohibited from giving them assault weapons?

Mr. REYES. Under State law—see, this, under the State law they cannot have automatic weapons.

Mr. SHAYS. Under every State or in some States, or in every State?

Mr. ZIMMERMAN. Some States have changed.

Mr. REYES. Recently. Very recently.

Mr. SHAYS. See, the logic of the assault weapon ban is that we want the law enforcement folks and the security people to have every advantage possible. We don't want the bad folks to have weapons that our people don't have.

Mr. REYES. We agree.

Mr. SHAYS. I mean, the government's got it screwed up here.

Mr. ZIMMERMAN. The legislation that we proposed would allow the security officers to use automatic weapons. Right now they are using semi-automatic weapons.

Mr. SHAYS. I want you to use whatever the hell you need to do the job. You know, our job in government is to make sure it's never a fair fight. We want our military people to always have the best.

Mr. ZIMMERMAN. I couldn't agree with you more.

Mr. TIERNEY. Would the gentleman yield on that for 1 second? The problem is these are not military people and these aren't public forces on that. The question I would have is, who is doing the background check on these individuals? Who are they? How well trained are they? And how confident can we be that they can be entrusted with this kind of weaponry and are going to do the job that we might normally expect of our own forces?

Mr. ZIMMERMAN. The background checks on the security officers is extremely aggressive. They are viewed to be in what's called a "critical group" because of recognizing that if they were the insider, what damage they would be able to cause. So there is a significant background check and behavioral observation that takes place. The vast majority of these individuals are prior military or law enforcement.

But the answer to your question, there is a very significant and appropriate background check being done.

Mr. TIERNEY. By the NRC?

Mr. ZIMMERMAN. Well, no. We work through the FBI. We pass the information to various agencies that have a variety of data bases that you are aware of, and those names are provided to those data bases. We are a passthrough.

Mr. REYES. Similar to a clearance, the fingerprinting and review will be done by the FBI. It's not the licensee if that's what you're asking.

Mr. SHAYS. Let me claim my time again. But I do think the gentleman is right on target. My biggest fear is the person who does have the weapon on the inside. I think one individual like that could practically accomplish whatever task they want. And so I think that is a key factor the gentleman has identified.

The bottom line is you are going to be looking at whether to revise your new design basis threat. How long would that take, though, if you then decided to do that?

Mr. REYES. Once we present that to the Commission, typically within a few weeks they make a decision one way or the other. So then if they were to make a change, we will have to implement it through orders or some mechanism like that.

Mr. SHAYS. So how long would that take before it actually were met in the field.

Mr. REYES. It depends on the size of the increase. If you are talking about the number of adversaries——

Mr. SHAYS. Just give me a sense. Are we talking a year more?

Mr. REYES. That should be in months we can issue the orders, and then the implementation will take a little bit longer, depending on the magnitude.

Mr. SHAYS. A little bit longer means what? A year?

Mr. REYES. My guess would be a year.

Mr. SHAYS. No, no. See, that isn't a little bit longer. I don't feel like there is an intensity level at NRC, I honestly don't. But we will get to that later. I think we need to get to the next.

Ms. WATSON. Is this just a followup, or can it wait when they come back to us?

Mr. TURNER. This panel is going to be returning after panel two. Will you be able to stay for——

Ms. WATSON. Yeah. It was just pertinent to——

Mr. SHAYS. I would be happy to.

Ms. WATSON. I was just going to say what is really bothering me at this moment is that I represent a State that has a very porous border, and there are people coming across the Mexican border into the United States that are going to be able to buy automatic assault weapons in their corner sporting goods store because the ban has evaporated. And I understand that there is a constant movement across our border, our southern border into the United States, where these people can go in with fictitious names and somebody else's ID and pick up one of these assault weapons. This will impact on you greatly, and so I just throw that out.

Mr. TURNER. Perhaps when they return that's an issue they can address at that time, if that's OK.

Ms. WATSON. That's fine. So just keep that in mind, my concern.

Mr. TURNER. What I understand is that panel one is going to remain while panel two testifies, and then return to us for additional questions after we have heard the testimony of Mr. Jim Wells. So we will excuse you at this point, with the understanding that you are going to be remaining.

Mr. SHAYS. And we thank you for that. That will be helpful.

Mr. TURNER. And then we will call forward panel two, which is Mr. Jim Wells, Director, National Resources and Environment Government Accountability Office, who will be accompanied by Mr. Raymond H. Smith, Jr., Assistant Director, and Mr. Kenneth E. Lightner, Jr., Senior Analyst.

Gentlemen, we do swear in our witnesses for the hearing. If you would please stand and raise your right arm.

[Witnesses sworn.]

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

Mr. TURNER. We welcome you, Mr. Wells, and look forward to your testimony.

STATEMENT OF JIM WELLS, DIRECTOR, NATURAL RESOURCES AND ENVIRONMENT, GOVERNMENT ACCOUNTABILITY OFFICE, ACCOMPANIED BY RAYMOND H. SMITH, JR. ASSISTANT DIRECTOR; AND KENNETH E. LIGHTNER, JR., SENIOR ANALYST

Mr. WELLS. Thank you, Mr. Chairman. We are pleased to be here today to discuss NRC's efforts to improve security at the Nation's 104 commercial nuclear power plants. Today, it's 3 years after the Twin Towers and Pentagon attacks, and we are discussing what NRC has done, where they are, and what's left to do. To NRC's credit they responded immediately, advising the plants to go to the highest levels of security, and they issued about 60 advisories and orders.

As an auditor, I am going to stop here and let them take credit for what they've done. They have, in fact, done a lot of things, and there is no doubt that security has been enhanced. But what we get paid to do as auditors is to bring forth concerns, and that's what I will do today.

While we applaud these efforts, the question is today: Has it been enough? It will take several more years for NRC to make an

independent determination that each plant has taken responsibile, reasonable, and appropriate steps to provide protection.

The first step that NRC chose was to create new security plans to implement their new DBT. While the original plan was envisioned to take 2 years, the commissioners decided to use an industry-developed template with yes-and-no answers to speed up the process. And, Mr. Tierney, they did hire contractors to help review the plans, and they wanted to get it done in 6 months.

Now, we have some concerns about how the NRC is doing this first step. Not that this first step is wrong, it's just the process they chose to use.

First, NRC's review has been rushed, and is largely a paper review, in our opinion. NRC reviewers are generally not visiting the plants to obtain details. However, we have learned that they are recently beginning to visit some of the plants and ask some questions relating to their plans. We understand they may have visited about approximately 4 or 5 of the 65 facilities and the 100 plants that are under consideration.

The plans themselves, and we have reviewed 12 of those plans, do not detail defensive positions at the site, how the defenders would be deployed to respond to that attack, or how long the deployment would take. In addition, NRC is not requesting the documents and the studies supporting the plan; so, in our opinion, as a result, NRC today as they are reviewing these plans, even though when they are approved they still will not have a lot of detailed knowledge about the actual security at the individual facilities prior to the approval of those plans.

Second, as it clearly has already been pointed out, it will take up to 3 years for the NRC to test these plans through force-on-force exercises at each facility. Moreover, NRC is considering action that could potentially compromise the integrity of these exercises. And I refer, as members of the subcommittee have already raised, the consideration of using a private company, Wackenhut, that is a company that the nuclear industry has selected, a company that clearly has had problems in the past at Oak Ridge—and, I might add, that NRC was doing oversight when these problems did happen—and a company that provides guards for about half the facilities to be tested. We understand Wackenhut is currently under contract with about 50 percent of the nuclear facilities.

This relationship with the industry also raises questions about the force's independence. And that's just a question that needs to continue to be asked in terms of due diligence by the NRC in terms of assuring that whatever contractor is used, that there is independence.

We note that the NRC's DBT is similar to DOE, as you have stated, Mr. Chairman and Mr. Shays. As you know, in April 2004, DOE officials told this subcommittee that they would have to rethink its threat assessment that they were using. DOE, we understand, completed that review last Tuesday and substantially increased their DBT.

If the NRC, when they consult with their commissioners, decides to revisit or revise the DBT, NRC will clearly need more time. How much time I think is a good question, that's already been asked of the NRC.

Also, funding the cost of any additional protection that may be required could also be a fairly significant issue for the industry. NRC has already clearly publicly stated that the current DBT that they are being required to defend against is the largest reasonable threat against which a regulated private guard force should be expected to defend under existing law. Also, potential vulnerabilities of additional assaults are on the horizon and currently are being addressed outside of the existing DBT. Any change in any of these approaches could place additional requirements on the plants. And I speak here about the airborne nature over the nuclear power plants.

In conclusion, can the public be assured that NRC's efforts will protect the plants against attack? Our answer to you today is not yet. It will still be some time before NRC can provide the public with full assurances that what has been done is enough. Some of these enhancements are still being put in place, and they remain to be tested.

Ms. Maloney and Congresswoman Watson, you have raised questions about NRC not agreeing to do some of our recommendations. Yes, we still disagree. Maybe it's an issue of substantial versus minor. We've found, others have found, sleeping guards, guards that have falsified records; access has been granted to individuals in highly secured areas that had no business being there. We are not sure that's minor.

While NRC may initially disagree with some of the things that we raise about trying to improve, it's questions like this raised by this subcommittee that may help the NRC in terms of seeing the light and moving forward and making some substantial improvements.

We have a lot more audit work to do, Mr. Chairman. You have asked us to do a lot of things, including an assessment of the DBT and a lot of concern about the vulnerabilities, and is the current DBT actually going to do anything to help protect the actual vulnerabilities that exist. So we still owe you a report a year from now or early next year, if we can finish it, on how NRC defines the threat faced by the nuclear power plants. We believe, based on what we have seen today—understanding that we are still preliminarily still doing our audit, we have not completed our work, and, in fairness to the NRC, have not given them an opportunity to comment or react to what we have seen today—that it's important that NRC act quickly and take a strong leadership role in establishing a worthy adversary team for these upcoming exercises.

I can't overemphasize how important these exercises are to test what's being put in place. These improvements are expensive, and we want to make sure that they are actually doing what they are intended to do and can in fact defend the plants. Perhaps NRC needs to consider establishing priorities for the facilities to be tested.

Quite frankly, we have seen a common general approach that they take. They tend to look at plants in general, generically. But clearly when you come to vulnerabilities and you come to assessment of threats, you need to look much more closely and individually at plants and perhaps prioritize where you put your attention first. They need to carefully analyze test results if they detect any

shortcomings in the facility's security, and, perhaps most importantly, be willing to require additional security improvements as warranted or as discovered.

Mr. Chairman, this testimony, or the statement, provides our preliminary reviews. We'll be happy to respond to any questions you may have. Thank you.

Mr. TURNER. Thank you, Mr. Wells.

[The prepared statement of Mr. Wells 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, September 14, 2004

NUCLEAR REGULATORY COMMISSION

Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants

Statement of Jim Wells, Director
Natural Resources and Environment

GAO-04-1064T

September 14, 2004

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-04-1064T, testimony before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

NUCLEAR REGULATORY COMMISSION

Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants

Why GAO Did This Study

The events of September 11, 2001, and the subsequent discovery of commercial nuclear power plants on a list of possible terrorist targets have focused considerable attention on the plants' capabilities to defend against a terrorist attack. The Nuclear Regulatory Commission (NRC), an independent agency established by the Energy Reorganization Act of 1974 to regulate the civilian use of nuclear materials, is responsible for regulating and overseeing security at commercial nuclear power plants.

GAO was asked to review (1) NRC's efforts since September 11, 2001, to improve security at nuclear power plants, including actions NRC has taken to implement some of GAO's September 2003 recommendations to improve security oversight and (2) the extent to which NRC is in a position to assure itself and the public that the plants are protected against terrorist attacks.

This testimony reflects the preliminary results of GAO's review. GAO will issue a more comprehensive report in early 2005.

www.gao.gov/cgi-bin/getrpt?GAO-04-1064T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Jim Wells, (202) 512-3841, wellsj@gao.gov.

What GAO Found

NRC responded quickly and decisively to the September 11, 2001, terrorist attacks with multiple steps to enhance security at commercial nuclear power plants. NRC immediately advised the plants to go to the highest level of security according to the system in place at the time and issued advisories and orders to the plants to make certain enhancements, such as installing more physical barriers and augmenting security forces, that could be completed quickly to shore up security. According to NRC officials, their inspections found that the plants complied with these advisories and orders. Later, in April 2003, NRC issued a new design basis threat (DBT), which establishes the maximum terrorist threat that a facility must defend against, and required the plants to develop and implement new security plans to address the new threat by October 2004. It is also improving its force-on-force exercises, as GAO recommended in its September 2003 report. These exercises are an important agency tool to ensure that the plants' security plans are adequate to protect against the DBT.

While its efforts to date have enhanced security, NRC is not yet in a position to provide an independent determination that each plant has taken reasonable and appropriate steps to protect against the new DBT. According to NRC officials, the facilities' new security plans are on schedule to be implemented by October 2004. However, NRC's review of the plans, which are not available to the general public for security reasons, has primarily been a paper review and is not detailed enough for NRC to determine if the plans would protect the facility against the threat presented in the DBT. For example, the plans GAO reviewed are largely based on a template and often do not include important site-specific information, such as where responding guards are stationed, how the responders would deploy to their defensive positions, and how long deployment would take. In addition, NRC officials are generally not visiting the facilities to obtain site-specific information and assess the plans in terms of each facility's layout. NRC is largely relying on force-on-force exercises it conducts to test the plans, but these exercises will not be conducted at all facilities for 3 years. NRC's oversight of plants' security could also be improved. However, NRC does not plan to make some improvements in its inspection program that GAO previously recommended and still believes are needed. For example, NRC is not following up to verify that all violations of security requirements have been corrected or taking steps to make "lessons learned" from inspections available to other NRC regional offices and nuclear power plants. Moreover, if NRC needs to revise its DBT further as the terrorist threat is better defined, it will need longer to make and test all the necessary enhancements. The Department of Energy, for example, is currently reviewing the DBT for its nuclear facilities.

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss our ongoing review of the Nuclear Regulatory Commission's (NRC) efforts to improve security at the nation's 104 commercial nuclear power plants licensed to operate. These plants, which are located at 65 facilities in 31 states, provide about 20 percent of the nation's electricity.[1] We are conducting this review at your request and expect to issue our final report early next year.

The events of September 11, 2001, and the subsequent discovery of commercial nuclear power plants on a list of possible terrorist targets have focused considerable attention on the plants' capabilities to defend against a terrorist attack. However, as you know, NRC is not alone in the challenges it faces to protect against terrorism. Recently, the 9/11 Commission's report highlighted the accomplishments and challenges that remain on many fronts in the nation's fight against terrorism. In recent testimony before this Committee, the Comptroller General applauded the efforts of the 9/11 Commission and discussed its recommendations to improve information sharing and analysis by the intelligence agencies.[2] We have also testified several times before this Subcommittee on weaknesses in border security, federal action needed to address security challenges at the nation's chemical facilities, and the issues faced by the Department of Energy (DOE) in its efforts to secure its nuclear facilities.[3]

To protect commercial nuclear power plants from a terrorist attack, NRC formulates a design basis threat (DBT), which establishes the maximum terrorist threat that a facility must prepare to defend against. The DBT characterizes the elements of a postulated

---

[1] More than one nuclear power plant are located at some facilities.

[2] GAO, *9/11 Commission Report: Reorganization, Transformation, and Information Sharing*, GAO-04-1033T (Washington, D.C.: Aug. 3, 2004).

[3] GAO, *Border Security: Additional Actions Needed to Eliminate Weaknesses in the Visa Revocation Process*, GAO-04-899T, (Washington, D.C.: July 13, 2004); GAO, *Homeland Security: Federal Action Needed to Address Security Challenges at Chemical Facilities*, GAO-04-482T (Washington, D.C.: February 23, 2004); GAO, *Nuclear Security: DOE Must Address Significant Issues to Meet the Requirements of the New Design Basis Threat*, GAO-04-701T (Washington, D.C.: April 27, 2004); and 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).

attack, including the number of attackers, their training, and the weapons and tactics they are capable of using. Each facility must prepare a security plan describing its strategy for defending against the threat presented in the DBT. NRC is responsible for reviewing and approving these plans, inspecting the facilities to verify compliance with the plans and other NRC requirements, and conducting force-on-force exercises (mock terrorist attacks) at the facilities to ensure that the facilities' execution of their security plans could repel an attack. NRC considers the DBT and the security plans to be safeguards or sensitive information and does not make them available to the general public.

Our current review is the second on NRC's security program since the September 11 attacks. In our earlier report, issued in September 2003, we made a number of recommendations to NRC to improve its oversight of security at commercial nuclear power plants.[4]

In my testimony today, I will (1) describe NRC's efforts since September 11, 2001, to improve security at nuclear power plants, including actions it has taken to implement some of our September 2003 recommendations to improve security oversight and (2) discuss our preliminary views on the extent to which NRC is in a position to assure itself and the public that its efforts will protect the plants against terrorist attacks. To conduct this work, we reviewed the security advisories and orders NRC has issued to the facilities since September 11, 2001. We also reviewed security documents, such as the DBT and individual facilities' draft security plans,[5] and interviewed NRC security program officials. We did the work reflected in this statement from March 2004 through August 2004 in accordance with generally accepted government auditing standards.

In our final report, we will discuss the extent to which NRC is using a risk management approach to improve security at nuclear power plants. More specifically, we will report

[4] GAO, *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*, GAO-03-752, (Washington, D.C.: September 4, 2003).

[5] We reviewed 12 of the 65 facilities' draft security plans. According to NRC officials, the plans we reviewed were generally representative of all the plans.

on NRC's efforts to (1) define the threat faced by nuclear power plants, (2) identify and characterize the vulnerabilities that would allow a threat to be realized, (3) assess the risks and determine priorities for protecting the plants, and (4) identify the countermeasures to reduce the risk of a successful terrorist attack.

In summary:

NRC responded quickly to the September 11, 2001, terrorist attacks with multiple steps to enhance security at commercial nuclear power plants. For example, NRC

- immediately advised the plants to go to the highest level of security according to the system in place at the time;

- issued a series of advisories and orders to the plants to make certain security enhancements—such as installing additional physical barriers, augmenting security forces, increasing patrols, and further restricting plant access—that could be completed quickly to shore up security until a more comprehensive analysis of the terrorist threat and how to best protect the plants against that threat could be completed.

- issued a new DBT in April 2003 and required the plants to develop and implement—by October 2004—new security plans setting out how the plants will protect against the threat defined in the new DBT. NRC expects the plants will meet this deadline; and

- improved its force-on-force exercises, which are an important agency tool to ensure that the plants are secure, by planning to conduct the exercises every 3 years instead of every 8 years and to make them more realistic, which we had recommended.

While we applaud these efforts, it will take several more years for NRC to make an independent determination that each plant has taken reasonable and appropriate steps to protect against the threat presented in the new DBT. The plants' development and implementation of security plans to comprehensively address the new DBT is a critical step in ensuring that individual plants can defend against terrorism. Although new security plans are to be approved and implemented by October 29, 2004, NRC will not have detailed knowledge about security at individual facilities to ensure that these plans provide this protection. NRC will not have this detailed knowledge, primarily for two reasons:

- First, NRC's review of the new security plans has been rushed and is largely a paper review. NRC is conducting its review of the plans over a 6-month period—as the plants are implementing the plans—and NRC reviewers are generally not visiting the plants to obtain details about the plans and view how the plans interface with the plants' physical layout. For example, the plans do not detail defensive positions at the site, how the defenders would deploy to respond to an attack, or how long the deployment would take. In addition, NRC is not requesting, and the facilities are generally not submitting for review, the documents and studies supporting the draft security plans.

- Second, it will take up to 3 years for NRC to test implementation of the new plans through force-on-force exercises at all facilities. Moreover, NRC is considering action that could potentially compromise the integrity of the exercises. The agency is planning to require the use of an adversary force trained in terrorist tactics, as we recommended in our September 2003 report. However, NRC is considering the use of a force provided by a company that the nuclear power industry selected; this company provides guards for about half the facilities to be tested. This relationship with the industry raises questions about the force's independence. Furthermore, NRC is not taking advantage of other opportunities to improve the effectiveness of the exercises and its oversight in general by implementing other recommendations from our September 2003 report. For

example, NRC is not following up to verify that all violations it found in previous inspections have been corrected and is not taking steps to make "lessons-learned" from inspections available to other regional offices and nuclear power plants, as we had recommended.

In addition to these concerns, we note that NRC's DBT is similar to the DOE's DBT for its nuclear facilities. As you know, in April 2004, DOE officials told this Subcommittee that it would have to revisit its post-September 11 DBT. If NRC also decides to revisit and revise its DBT, NRC will need even longer to put all the necessary security enhancements in place and to test them. Funding the costs of the additional protection could also be an issue. NRC has already stated that the current DBT is the largest reasonable threat against which a regulated private guard force should be expected to defend under existing law. Also, certain potential vulnerabilities, such as airborne assaults, are currently being addressed outside of the DBT. Any changes in this approach to certain vulnerabilities could similarly place additional requirements on the plants.

Background

NRC is an independent agency established by the Energy Reorganization Act of 1974 to regulate the civilian use of nuclear materials. NRC's Office of Nuclear Security and Incident Response, which was established in April 2002, is primarily responsible for regulating and overseeing security at commercial nuclear power plants. This office also develops overall agency policy and provides management direction for evaluating and assessing technical issues involving security at nuclear facilities. In addition, it coordinates with the Department of Homeland Security, the intelligence and law enforcement communities, DOE, and other agencies on security matters.

NRC begins regulating security at a commercial nuclear power plant when the plant is constructed. Before granting an operating license, NRC must approve a security plan for the plant. If more than one plant is located at a facility, the licensee prepares a physical

security plan covering all the plants at the site. Since 1977, NRC has required facilities to have a security plan that is designed to protect against a DBT for radiological sabotage.[6] The DBT characterizes the elements of a possible attack, including the number of attackers, their training, and the weapons and tactics they are capable of using. Since it was first issued in 1977, the DBT has been revised twice, each time to reflect increased terrorist threats. The first revision occurred in 1993 in response to the first terrorist attack on the World Trade Center in New York City and to a vehicle intrusion at the Three Mile Island nuclear power plant in Pennsylvania.[7] The second revision was issued on April 29, 2003, in response to the September 11, 2001, terrorist attacks.

NRC oversees plant security through several activities, particularly security inspections and force-on-force exercises. In annual security inspections at all the plants, inspectors are to check that the plant's security programs meet NRC requirements for access authorization, access control, and response to contingency events. The inspectors also are to review changes to the plant's security plan and self-assessment of security. NRC suspended these inspections in September 2001 to focus its resources on the implementation of security enhancements from NRC's advisories and orders. NRC reinstated the inspection program in early 2004.

NRC began conducting force-on-force exercises under its security inspection program in 1991. The agency suspended these exercises, which were referred to as Operational Safeguards Response Evaluation (OSRE) exercises, after the September 11, 2001, attacks because they considered it unsafe to perform mock attacks during a period of heightened security and because NRC and licenses security resources were focused on responding to the events of September 11, 2001. NRC has conducted some exercises during 2003 and 2004 to gain the information necessary to initiate a revised, permanent force-on-force exercise program sometime in the near future. Although NRC officials have not

[6] Radiological sabotage against a nuclear power plant is a deliberate act that could directly or indirectly endanger public health and safety by exposure to radiation.

[7] On February 7, 1993, an intruder drove onto the Three Mile Island power plant site, through a gate, and crashed through a roll-up door into the turbine area. The intruder challenged security barriers and disrupted operations for 4 hours before he was apprehended.

decided on an exact date, they anticipate that the exercises will resume very soon after the facilities have implemented their security plans, which is scheduled for the end of October 2004.

NRC Actions Since September 11, 2001, to Improve Security at Nuclear Power Plants

Shortly after September 11, 2001, NRC began to respond to the heightened risk of terrorist attacks. Between September 11, 2001, and the end of March 2003, the agency issued over 60 advisories to licensees of nuclear power plants. These advisories recommended enhancements that could be made quickly to shore up security until a more comprehensive analysis of the terrorist threat and how best to protect the plants against the threat could be completed. NRC immediately advised the plants to go to the highest level of security according to the system in place at the time. It followed with advisories and orders designed to increase the size and improve the proficiency of plants' security forces, restrict access to plants, and increase and improve plants' defensive barriers. For example, on October 6, 2001, NRC issued a major advisory, recommending that the licensees take immediate action to increase the number of security guards and to be cautious about using temporary employees.

From October 2001 to January 2002, NRC conducted a three-phase security inspection, checking the facilities to see if they had implemented these advisories. In phase one, NRC inspectors used an NRC-prepared checklist to document the implementation status of NRC's October 6, 2001 advisory. In phase two, security inspectors conducted a more in-depth evaluation of the facilities' implementation of the advisories. During phase three, NRC's security inspectors reviewed each facility's security program to determine if it had complied with the additional measures recommended in the October 6, 2001, advisory. NRC concluded that all facilities were in compliance but that the facilities had not consistently interpreted the recommended measures.

NRC used the results from the three-phase inspection to develop a February 25, 2002, order requiring facilities to implement additional security measures by August 31, 2002.[8] Many of these measures had been recommended in previous advisories. NRC then conducted security inspections to verify facilities' compliance with all aspects of the order. The inspections were completed in December 2003, and NRC found that all nuclear power facilities were in compliance with the order.

NRC also acted on an item that had been a security concern for a number of years—the use of temporary clearances for temporary employees at the plants. Commercial nuclear power plants use hundreds of temporary employees for maintenance—most frequently during the period when the plant is shut down for refueling. In the past, NRC found instances in which personnel who failed to report criminal records had temporary clearances that allowed them unescorted access to vital areas.[9] In an October 6, 2001, advisory, NRC suggested that facilities limit temporary clearances for temporary workers. On February 25, 2002, NRC issued an order that limited the use and duration of temporary clearances, and on January 7, 2003, NRC issued an order to eliminate the use of temporary clearances altogether. NRC now requires a criminal history review and a background check investigation to be completed before allowing temporary workers to have unescorted access to the power plant.

NRC issued its revised DBT in April 2003 to reflect the post-September 11 terrorist threat. In January 2003, NRC developed a draft DBT that it sent to federal, state, and local law enforcement agencies, federal intelligence and counterintelligence agencies, and the nuclear industry for review and comment. Between January and April of 2003, revisions were made, and the revised drafts were sent for additional comments. On April 29, 2003, NRC issued an order requiring the facilties to protect the power plants from a terrorist attack fitting within the parameters of the new DBT. The new DBT reflected the

[8] NRC Order EA-02-026.

[9] The vital area, within the protected area, contains the plant's equipment, systems, devices, or material whose failure, destruction, or release could endanger the public health and safety by exposure to radiation. This area is protected by guard stations, reinforced gates, surveillance cameras, and locked doors.

increased size of a potential terrorist force, the more sophisticated weaponry, and the different methods of deployment demonstrated by the September 11 terrorist attacks. NRC stated that this new DBT was the "largest reasonable threat against which a regulated private guard force should be expected to defend under existing law." Licensees were given 1 year to develop new security plans based on the new DBT.

At the same time, NRC issued two other orders that (1) limited work hours for security personnel (to 16 hours per 24-hour period, 26 hours per 48-hour period, and 72 hours per week) so that excessive hours would not impair security forces in performing their duties and (2) required enhanced training and qualifications for the plants' security forces. All told, according to the Nuclear Energy Institute,[10] by the end of 2004, the nuclear power industry will have invested about $1 billion in security enhancements since September 11, 2001.

During this period, NRC also developed and strengthened its relations with other federal agencies. It collaborated with the Federal Aviation Administration on protecting airspace over the plants and worked with the Department of Homeland Security, Federal Bureau of Investigation, and local law enforcement agencies to monitor and analyze security threats and to determine additional security measures needed to meet such threats.

NRC has also taken, or is taking, steps to implement our September 2003 recommendations to improve its security inspections and force-on-force exercises. We had recommended that the NRC Commissioners ensure that the agency's security inspection program and force-on-force exercise program are restored promptly. NRC reinstated the security inspection program in February 2004.

NRC has not yet made force-on-force exercises a required activity, as we recommended, but it is taking steps in that direction. During 2003, NRC completed a "pilot" force-on-force program, which included 15 exercises. This pilot program was designed to

[10] The institute represents licensees of commercial nuclear power plants.

determine how future force-on-force exercises would be conducted. After completing the 15 pilot exercises, NRC summarized the results in a "lessons learned" document. NRC is now conducting "transition" force-on-force exercises to help it formulate a new, permanent program. Participation in both the pilot and most of the transition exercises was voluntary for the facilities. Only some of the pilot exercises tested the full DBT, and none of the transitional exercises have or will test the full terrorist capabilities of the DBT. NRC officials said that they will not start conducting exercises using the new DBT until November 2004, after the facilities have implemented their new security plans.

NRC is also making the following additional improvements we recommended for these exercises:

- conducting the exercises more frequently at each site—every 3 years rather than the once every 8 years schedule of the past;

- using laser equipment in all force-on-force exercises to more accurately account for shots fired and to establish a more realistic setting;

- continuing the practice, begun in 2000, of prohibiting licensees from temporarily increasing the number of guards defending the plant and enhancing plant defenses for force-on-force exercises, or requiring that any temporary security enhancements be officially incorporated into the licensees' security plans; and

- requiring the exercises to make use of the full terrorist capabilities stated in the DBT, including the use of an adversary force that has been trained in terrorist tactics.

NRC Cannot Yet Provide Assurances That Its Efforts Will Protect Nuclear Power Plants Against Terrorist Attacks as Outlined in the New DBT

As the principal regulator of commercial nuclear power plants, NRC has an important responsibility to provide an independent determination that each plant is protected against the threat presented in the new DBT. While its efforts to date have no doubt enhanced security, NRC cannot yet provide this determination for three principal reasons. First, its review of the facilities' new security plans setting out how the facilities will respond to the threat presented in the new DBT is not detailed enough. Second, it will not test the effectiveness of all the plans and security at all plants with force-on-force exercises for 3 years, and it does not plan to make some improvements in its security oversight that we believe are needed and have previously recommended. Third, NRC could potentially need to further revise its DBT as the terrorist threat is better defined, which could require changes in the security plans and additional security improvements.

NRC's Review of Security Plans Is Not Detailed Enough to Determine if They Effectively Address the New DBT

NRC's strategy for reviewing the facilities' security plans generally allows for only a document review. While NRC staff originally estimated that it would take 2 years to review the plans, NRC now expects to take 6 months—from April 29, 2004, through October 29, 2004—to review and approve the facilities' security plans. The facilities are also expected to have their plans implemented by that date.

To review the plans in 6 months, NRC assigned 20 NRC staff and contracted for 20 staff from DOE's Idaho National Engineering Laboratory to perform the reviews. The facilities' use of an industry-developed template is also expected to help speed the review.[11] The template was intended to provide standard language for about 80 percent of the plans' contents. However, the plans we reviewed relied almost entirely on the template language and provided little facility-specific information.

[11] NRC provided input to the template's development.

Agency officials are generally not visiting the facilities to obtain site-specific information and assess the plans in terms of each facility's particular layout. Since completion of our work, NRC has decided to visit six or seven of the plants to verify information in the plan; however, it will not visit the vast majority of plants. In addition, the plans do not contain much detail. For example, the 12 plans NRC provided for our review do not include information about where responding guards are stationed, where their defensive positions are located, how the responders would deploy to their defensive positions, and how long deployment would take.[12] The plans state that "[p]hysical security measures and specific response protocols for the onsite security force are contained in facility implementing procedures." Also, in all the plans we reviewed, the defensive positions are described only as being established "where necessary." None of the plans we reviewed specified the type of weapons the security forces will carry; stating only that the forces will meet NRC's minimum requirements. According to staff from our Office of Special Investigations with experience in law enforcement and physical security, the security plans are, at best, general guidelines.

The plans often refer to other documents that detail how the requirements will be met and how the plans will be implemented. However, because of the 6-month review time frame, NRC officials do not plan to review these supporting documents as part of their approval process. According to NRC officials, the principal purpose of the plans is to commit the facilities to comply with all NRC security regulations and the template-based plans accomplish that purpose for about 80 to 90 percent of the information.

NRC's Security Oversight Is Limited by Timing of Key Activities and Inaction on Some of Our Recommendations

NRC will not determine the adequacy of the sites' procedures and programs for implementing their security plans and the sites' ability to actually implement the plan until it conducts inspections and force-on-force exercises at the sites. Because NRC

[12] Staff from our Office of Special Investigations with experience in law enforcement and physical security assisted in reviewing these plans.

plans to annually inspect all sites and conduct force-on-force exercises on a 3-year cycle, it could be 2007 before NRC can say with assurance that all the sites can be protected from a terrorist attack as presented in the new DBT.

In addition to the limitations of the security inspections and the timing of the force-on-force exercises, NRC has not implemented some of the recommendations we made in our September 2003 report to improve its oversight. We recommended that the NRC Commissioners

- require that NRC regional inspectors conduct follow-up visits to verify that corrective action has been taken when security violations, including non-cited violations,[13] have been identified;

- ensure that NRC routinely collects, analyzes, and disseminates information on security problems, solutions, and lessons learned and shares this information with all NRC regions and licensees; and

- enforce NRC's requirement that force-on-force exercise reports be issued within 30 to 45 days after the end of the exercise to ensure prompt correction of the problems noted.

Implementation of these recommendations is needed to correct some important program limitations. For example, during annual inspections, NRC inspectors often classified security problems as non-cited violations if the problem had not been identified frequently in the past or if the problem had no direct, immediate, adverse consequence at the time that it was identified. Instances of a security guard sleeping on duty and a security officer falsifying logs to show that he had checked vital areas and barriers when he was actually in another part of the plant, for example, were treated as non-cited violations. This classification tends to minimize the seriousness of the problem. Non-

[13] A non-cited violation is a problem that had not been identified more than twice in the past year or had no immediate, direct consequences at the time it was identified.

cited violations do not require a written response from the licensee and do not require NRC inspectors to verify that the problem has been corrected. NRC used non-cited violations extensively for serious problems, thereby allowing the licensees to correct the problem on their own without NRC verification of the correction. Consequently, we believe NRC may not be fully aware of the quality of security at a site, and the lack of follow-up and verification reduces assurances that needed improvements have been made.

NRC also has not created a system to share the security problems, solutions, and lessons learned that it finds during security inspections with all the NRC regions and licensees. NRC did create a management review panel that is tracking the regions' findings during the security inspections and the dispositions of the findings. It is also keeping a database of all the findings and dispositions or solutions; however, the database is not accessible by the regions and licensees.

With respect to NRC's enforcement of its requirement for force-on-force exercise reports, NRC officials said they do plan to issue reports when the permanent force-on-force program is reinstated, but the reports will not be made public. During the pilot force-on-force exercises, NRC did not issue any reports, although it prepared a "lessons learned" document for the Commissioners. In addition, an NRC official stated that NRC will not issue reports on the new transitional force-on-force exercises, but will prepare another internal lessons learned document. We continue to believe that NRC needs to promptly issue reports on each exercise to ensure that any security problems are quickly corrected. These reports would also provide the documentation needed to assess trends and patterns among facilities as well as at particular facilities over time.

Finally, although NRC is taking action—as we recommended in our September 2003 report—to establish an adversary force trained in terrorist tactics, NRC is not establishing the force in a manner that provides confidence that the force will be independent and highly trained, and will endeavor to find weaknesses in the facilities' security. NRC delegated the task of establishing the adversary force to an organization—

the Nuclear Energy Institute—that represents the licensees of nuclear power plants. The company the Institute selected currently provides security guards to about half of the nuclear power sites to be tested. The company's relationship with the industry raises questions about the force's independence. Of further concern, this company was recently involved in a controversy over similar tests. During a June 2003 DOE force-on-force exercise at a nuclear site in Oak Ridge, Tennessee, security guards working for this company received uncharacteristically high scores. A subsequent investigation by DOE's Office of the Inspector General indicated that the guards might have cheated on the test and perhaps on many other tests at Oak Ridge, dating back to the mid-1980s. It was alleged that the guards had studied plans for the simulated attacks before they were carried out, had disabled the laser sensors they wore during tests to determine when they were "shot" by mock enemies, arranged trucks and other obstacles to help foil simulated attacks, created special, nonstandard plans to help them perform better on tests, and put more guards on duty at the time of the tests than would normally have been present.

If NRC Needs to Revise Its DBT, Additional Security Enhancements Could Be Required

In April 2004, DOE told this Subcommittee that it would have to review its post-September 11, 2001, DBT for its nuclear facilities to determine if it should be more stringent.[14] If NRC decides, as it gains a better understanding of the terrorist threat, that it also needs to reconsider its DBT, it could take longer to put all necessary enhancements in place and test them with force-on-force exercises. Depending on the additional enhancements needed, funding of the costs of the additional protection and how quickly it could be put in place could also become an issue. NRC previously stated that its April 29, 2003, DBT is the largest reasonable threat against which a regulated private guard force should be expected to defend under current law.

[14] DOE's post-September 11, 2001, DBT, which is similar to NRC's in terms of the threat it outlines, was issued in May 2003. DOE has not yet completed its review of the DBT.

Similarly, NRC is addressing certain potential vulnerabilities outside of the DBT. For example, the terrorists' use of aircraft on September 11 raised questions about nuclear power plants' vulnerabilities to such attacks. According to NRC, although the design of many facilities considered the probability of accidental aircraft crashes that may pose undue risks to public health and safety, only a few facilities were specifically designed to withstand an accidental impact. Nonetheless, NRC believes that nuclear power facilities are among the most hardened industrial facilities in the United States. They are massive structures with thick exterior walls and interior barriers of reinforced concrete designed to withstand tornadoes (and projectiles propelled by tornadoes), hurricanes, fires, floods, and earthquakes. NRC also believes that the efforts to enhance security at airports and on airplanes and to identify potential terrorists and prevent potential attacks before they occur are an important part of reducing the threat of airborne attacks.

After the September 11 attacks, the Federal Aviation Administration, working with NRC, advised pilots to avoid the airspace above or in proximity to all nuclear power facilities and not to circle in their vicinity. NRC also undertook a major classified research and engineering effort, in conjunction with national laboratories, to evaluate the vulnerabilities and potential effects of a large commercial aircraft's hitting a nuclear power site. This effort includes consideration of additional preventive or mitigating measures to enhance the protection of public health and safety in the event of a deliberate aircraft crash into a nuclear power plant or spent (used) nuclear fuel storage facility. The results are classified and cannot be discussed in this open hearing. According to NRC officials, certain types of aircraft hitting facilities at certain locations pose some risks. The officials noted that, in these cases, the plants would have enough time to take advantage of certain safety features to substantially lessen the risks. NRC officials also believe that the plants would have sufficient time to implement emergency preparedness plans, if necessary.

Airborne assaults on plants remain a public concern. If further consideration of NRC's aircraft study results lead to changes in NRC's approach, the DBT may need to be revised further, again raising questions about the timing and cost of improvements.

- - - -

In closing, the nation's commercial nuclear power plants are no doubt more secure against a terrorist attack now than they were on September 11, 2001. NRC responded quickly and decisively to the attacks by requiring various enhancements to existing security at the plants. It will be some time, however, before NRC can provide the public with assurances that what has been done is enough. Some of these enhancements are still being put in place, and NRC cannot independently determine that the enhancements will adequately secure the facilities until they have been effectively tested with force-on-force exercises. While our assessment of NRC activities is still underway, we believe that it is important for NRC to act quickly and take a strong leadership role in establishing a worthy adversary team for these exercises, establish priorities for the facilities to be tested, carefully analyze the test results for shortcomings in facility security, and be willing to require additional security improvements as warranted.

Mr. Chairman, this testimony provides our preliminary views. We would be happy to respond to any questions that you or Members of the Subcommittee may have.

For further GAO Contact and Staff Acknowledgements

For further information on this testimony, please contact Jim Wells at (202) 512-3841 or at Wellsj@gao.gov. Raymond H. Smith, Jr.; Kenneth E. Lightner, Jr.; Jill Ann Roth Edelson; Kevin L. Jackson; Carol Herrnstadt Shulman; and Barbara R. Timmerman made key contributions to this testimony.

(360393)

Mr. TURNER. One of the statements in your written testimony, it says NRC has already stated that the current design basis threat is the largest reasonable threat against which a regulated private guard force should be expected to defend under existing law.

Now, we have been looking at, in addition to power plants, nuclear weapons facilities, and it has seemed to me that perhaps we are going about this backward. The design basis threats are being defined as a result of the resources that are available rather than the actual threat that exists. The statement that you have here in your testimony seems to indicate that the design basis threat is not a full evaluation of what the actual attack method or threat could be to a nuclear power plant, but is instead a review of what resources they have and what maximum capability that they would have to respond. Could you speak about that for a moment?

Mr. WELLS. Yes, sir. NRC in their own words have characterized their responsibility as a regulator which presents challenges, and they have used the word "balance." They have a lot of concern for balance in terms of what should be required, what can be regulated. And they also have a responsibility to maintain a viable industry to deliver electricity to this country. Clearly, that involves choices and decisions.

Our observation, having conducted several audits and continuing with our work, is that the NRC, as a regulator, has placed a lot of faith in what the licensees tell them. They also have to provide some trust level to the licensee. We have seen examples in doing our Davis-Besse work where that may not have been as valid as they should have been.

So I think the question being asked today and the question that continually needs to be asked: What do you expect of the regulator?

Mr. TURNER. The paragraph that I'm referring to goes on to say that, also, certain potential vulnerabilities such as airborne assaults are currently being addressed outside of the DBT.

Now, what it has seemed to me in reviewing the materials, that there is certainly—the responsibility for it is assigned outside of the design basis threat, but I'm not confident that it's currently being really addressed. Do you see any efforts that, outside the design basis threat, that there is coordination, that there is sufficient effort to actually respond to the threats that are beyond the box that they are currently dealing with with the design basis threat of the private guard force?

Mr. WELLS. Congressman Turner, NRC has given us access to the design basis threat. We are well aware of what the design basis threat, what is contained in the design basis threat. We are dealing with safeguarded security information that prevents me from actually discussing in terms of what is actually in the plan or not in the plan. We have asked them what they are doing in terms of considering airspace over the nuclear power plants. They have responded to us that they have contracted for, paid for, and have the results of a fairly significant study that they have done. They indicate it's classified. I cannot get into that today.

Mr. TURNER. I'm not asking about any information for you to disclose. I'm asking about the issue of coordination. It seems to me that the initial statement that we have in your written testimony

is the design basis threat is a box that is based upon a private guard force and that they are not necessarily going beyond that.

Then the next statement in the testimony is that with respect to airborne assaults and certainly, I would think, other issues that go outside of that box and what the private guard force would be able to do, which would require coordination with the DOD, we have also discussed NORTHCOM and NORAD. Do you see any evidence that coordination is effectively occurring, or is it just, as you relate, to other reviews, just a paper coordination going on?

Mr. WELLS. Let me respond that, as I said earlier, we are still conducting our work, we are still asking questions. I don't have a conclusion or a reaction for you. Factually, we are aware—as NRC stated this morning, they are talking to the FAA. We are aware that the nuclear industry themselves is on public record saying that is a defense that they don't believe is their responsibility, that is a national responsibility.

So we will continue looking at and assessing the requirements that are in the DBT or not in the DBT. That is something we haven't done yet.

Mr. TURNER. One real quick followup question. In the testimony that we heard before, it was dismissed as to whether or not aircraft attacking these facilities are of any danger. That doesn't seem reasonable to me. What is your opinion of that?

Mr. WELLS. We had several words in our statement that was sent to the NRC for classification purposes, and those sentences and words were removed from the statement because of the security concern. They do have information on the study that they have conducted.

Mr. TURNER. It is an area that you are concerned with then also?

Mr. WELLS. Absolutely. We will continue our assessment of the vulnerability versus the design basis threat that's being put up against it.

Mr. TURNER. Thank you, Mr. Wells.

Mr. Kucinich.

Mr. SHAYS. Would the gentleman yield for a second?

Mr. KUCINICH. Sure.

Mr. SHAYS. This is the statement you were going to give today?

Mr. WELLS. That's correct.

Mr. SHAYS. Were there a lot of things taken out of your statement?

Mr. WELLS. No, there was not. There was a few word adjustments. We sent the entire statement, from my opening statement to the end of my statement, for classification review because we have a public obligation——

Mr. SHAYS. I think that makes sense. That's not the issue. I just was curious if there was just one area.

Mr. WELLS. The area involved the airborne attack issue.

Mr. SHAYS. OK. Thank you.

Mr. TURNER. Mr. Kucinich.

Mr. KUCINICH. Thank you.

Mr. Wells, as Secretary of Energy, Secretary Abraham recently announced the formation of an elite specialized military-type team that would be used to test security at DOE facilities. Do you believe the NRC should follow suit and turn this function from what

you have described as sleeping intoxicated guards into a government function?

Mr. WELLS. Unfortunately, I haven't done the audit work to support a conclusion to give you a straight answer. I know that's something that this chairman has asked us to continue to do and report on the end of this year, and we are continuing.

Mr. KUCINICH. Well, you have done the audit work on one part of the equation.

Mr. WELLS. Yes, we have, but not on the design basis threat. But clearly we are aware that there are different types of facilities. There is nuclear material. We are aware that the DOE has different classifications of types of material and different guard force versus private guard force. There are different issues between the agencies that could account for some differences between what's required. We just don't know how valid that fact is until we actually have a chance to look at it.

Mr. KUCINICH. I want to go over some territory here. You stated in your testimony that the October 2004 deadline for implementing the DBT is on schedule, but that this is based only on a paper review, and that the NRC cannot determine if the plans would actually protect the facility against the threat presented in the DBT.

Mr. WELLS. That's correct, sir.

Mr. KUCINICH. Is that correct?

Mr. WELLS. That's correct. We know that they are 85 percent complete with approving those or looking at those plants. But even when they are 100 percent approved, we still take our position that they only got what they got.

Mr. KUCINICH. Well, so then should the NRC be more involved in the oversight over the DBT implementation process?

Mr. WELLS. Absolutely. They have acknowledged to us that this is a first step, and they have step two and step three and step four. We just know it's going to take additional time before they can reach that assurance to the public that everything that has been put in place will work.

Mr. KUCINICH. And what kind of improvements has GAO recommended to be implemented in the NRC inspection program, and, why if they have, has the NRC resisted in making those changes?

Mr. LIGHTNER. There are two open points from our report from last September that NRC has not taken action on. I believe they have been discussed earlier. But the one has to do with followup on security violations that were noted. Particularly we're concerned with something called noncited violations which are followed up by NRC only as part of a sampling process. And as stated earlier, I believe our difference with them is over what is significant and what isn't.

NRC cites these as noncited violations primarily because they have occurred less than two times in the prior year. I believe our concern is that even if they occur once, and they are significant, such as falsifying records related to guards' checkpoints or a sleeping guard, that they are significant and should be followed up on in every case to make sure that this doesn't happen in the future.

Mr. KUCINICH. So you then challenge the underlying assumption which the NRC has about what's significant?

Mr. WELLS. That's correct.

Mr. KUCINICH. And let's go a little bit deeper into this. Are you saying that their assumptions contain within them potential threats to the security of nuclear power plants?

Mr. WELLS. Noncited violations, if a guard is sleeping or unauthorized individuals are allowed access in secured areas, falls directly in security. I don't know how else to say that.

Mr. KUCINICH. So is that a yes?

Mr. WELLS. It certainly raises concern. Yes.

Mr. KUCINICH. Thank you.

Mr. TURNER. Ms. Watson.

Ms. WATSON. I'm going to quote from some information in your report, and you can tell me if it's accurate or not. And it says, for example, the plans do not detail defensive positions at this site, how the defenders would deploy to respond to an attack, or how long the deployment would take. In addition, NRC is not requesting and the facilities are generally not submitting for review the documents and studies supporting the draft security plans.

Can you comment on that?

Mr. WELLS. The best way to comment would be to describe a plan; a plan is approximately 150 pages long for a single plant; 80 to 85 percent of the information is a template in which the licensee responds and checks a box yes or no.

An example is the requirement that lighting be sufficient so that guards can see someone at night? The licensee would respond, yes, we have lighting.

I know I'm oversimplifying this a little bit, but I'm giving you the implication of the template nature of the plan that's developed. Basically, what the licensee is doing is certifying to or committing to the NRC that, when they get out there to look, with all the details, they will find that the licensee is committing that they will have something in place that will meet all the template requirements that NRC is imposing.

That's the nature of the plan that we've looked at. It does not describe where the guard tower is, the location of the guard tower. It does not describe that. It just says we have guard towers.

Ms. WATSON. Yeah, but they might be in New York City, you know. I'm not comfortable with where we are now, and I definitely am not comfortable with my constituents' security. And within the State we do have nuclear power plants.

Are you, as an agency that goes in and accounts for resources and so on, satisfied that we are where we need to be at this time, this point in time?

Mr. WELLS. In regard to the Nuclear Regulatory Commission?

Ms. WATSON. Yes.

Mr. WELLS. We have issued two reports. We are going on our third report. And in each of those reports we have surfaced concerns and made recommendations that we suggest could improve government operations and regulatory issues with the NRC. So we are doing what we can to raise these issues and to recommend fixes.

Ms. WATSON. But are you satisfied with where the NRC is? This is September 2004. Are you satisfied, September 2004, that we are where we should be?

Mr. WELLS. NRC needs to be given a lot of credit. They have done a lot of things as quickly as they possibly can under their requirements. I have to be careful in answering that personally, I would always like things to be done faster. And I agree with the chairman to say that 14 months to design the DBT, allowing another year to put it in place, seems like an awful long time. But we are dealing with a regulatory agency that has public concerns; they are facing lawsuits about whether they do rulemaking, whether they do orders.

I understand the challenge they have. Personally, I would hope that the intensity level, as the chairman referred to, perhaps could be moved forward. I encourage the NRC to ask the DOE why they were able to do a revision to their DBT so quickly. And in lessons learned, if there is something DOE did that the NRC could use, I would suggest that they pay attention and try that.

Ms. WATSON. And let me just say that I heard the word "resources," but I didn't hear the elaboration. Are they lacking the resources to work in a more speedy fashion?

Mr. WELLS. Clearly, the NRC has gotten a mandate and a mission to be a regulatory agency that is a commission that's funded by the industry. So there has always been this fine line between, we have an obligation to require our regulators to regulate an industry and how to go about doing that. There has always been resource constraints and issues involved with the NRC in terms of how much resources they have to effectively get the job one. And it's a very tough balance that they face.

Ms. WATSON. See, that kind of gives us a hint as to what we as policymakers, hello, who have the oversight, should be doing. And we, working with industries, nongovernmental, you know, ought to realize that they are not going to move unless they have the resources necessary.

So thank you for your statement. And I will yield back the balance of my time.

Mr. TURNER. Mr. Chairman.

Mr. SHAYS. Thank you.

I think you are being very fair to the NRC. I mean, you said they responded quickly and decisively to the September 11, 2001 terrorist attacks, and multiple steps to enhance security at commercial and nuclear plants. It gives, to me, more credibility when you point out some of what they aren't doing.

I do think there is some value in looking at parallels between what DOE is doing. What I'm getting a feeling of—and I would love you to explain this concept of orders versus rulemaking. The Secretary of Energy can basically say, damn it, just do it. And, you know, admittedly bureaucracies take a while, but doesn't the NRC have the capability to say let's do it? No more 2 years, no more whatever, just get the job done and do it quickly. Do they not have that capability?

Mr. WELLS. Mr. Chairman, I'm not a lawyer, but I believe that they do have wide discretion in orders that they can issue, advisories that they can issue. There is a line between what's voluntary implementation by the industry and what's required of the industry. However, I do know that they are facing several lawsuits challenging the right to issue just-do-it orders.

Mr. SHAYS. By these companies?

Mr. WELLS. By public interest groups.

Mr. SHAYS. Well, by public interest groups that are unhappy that they are not moving quickly. Are the companies taking challenges to the——

Mr. WELLS. I'm not sure who the——

Mr. SHAYS. Well, I mean, with all due respect, I mean, I might be one of those people going after the NRC as well if they are not moving quickly. I mean, we are really talking 6 years from September 11th to when the design basis threat is going to be shown at least in one experience at each plant. So your basic point to us is that this is pretty much a paper review today. Do you stand by that?

Mr. WELLS. I do. Step one has been a paper review.

Mr. SHAYS. I mean, there isn't any real-life stuff going on to make sure it's happening yet.

Mr. WELLS. We have been recently made aware that they visited four or five places to ask some questions about what was actually in the document.

Mr. SHAYS. Well, we have 65 places they could visit, and they have gone to four or five places?

Mr. WELLS. That's correct.

Mr. SHAYS. So, I mean, we are not even talking about the efforts to break the integrity of the plant and those exercises; we are just talking the NRC just going there and checking it out firsthand.

Mr. WELLS. That's correct.

Mr. SHAYS [presiding]. OK. So they are going to rely on the force-on-force, but they haven't started that yet.

Now, what I think is pretty stunning is your statement on page 13, where you talk about instances of security guards sleeping on duty and security officers falsifying logs to show that it's been checked—had checked vital areas and barriers when he was actually in a part of the plant, for example—were treated as non-cited violations. The whole issue of non-cited violations that was raised by my colleague, who gets to decide whether they are noncited violations?

Mr. WELLS. The NRC.

Mr. SHAYS. Now, what would be the logic for making them noncited? Tell me the logic. What would be their argument?

Mr. LIGHTNER. In a NRC letter responding to our last report, they wrote to us, "the use of noncited violation contributes to an environment that fosters licensee's self-identification and correction of problems, an important organizational behavior that NRC encourages."

It's our understanding that this is the philosophy that they have and that they want the licensee to identify and correct the problems that——

Mr. SHAYS. So you think if they make them cited, they won't do it? They won't share it? I'm missing the logic.

Mr. LIGHTNER. I believe it's a difference in philosophy between maybe NRC and the GAO.

Mr. SHAYS. Well, we'll have them explain the philosophy.

Mr. LIGHTNER. Based on these statements and their response to our report, I believe they believe that it's the responsibility of the

licensee—they would like the licensee to find as many problems as they can and correct them. And we wouldn't disagree that's a good thing for them to be the people onsite to find and correct them.

Mr. SHAYS. So what I'm reading in that is if they cite them, they will be less inclined to share them and disclose them?

Mr. LIGHTNER. No, I don't think so. I think they just want them to be aware of the problems and correct them. Our view is that's fine, except we believe a regulator should be aware of what the problems are and be right on top of the correction and followup on those to make sure they do the job.

Mr. SHAYS. So we basically have a grade; it's either cited or noncited. It's either a pass/fail? I don't mean pass/fail, I mean, a cited violation evidently is significant.

Mr. WELLS. It is significant, and they would do followup and they would verify in fact that it's been corrected. If it's a noncited violation, they would trust and have faith that the contractor has said I fixed it, and then the NRC would not necessarily do a followup to verify. They may do some sampling a year so later to see if it was.

Mr. SHAYS. Is that because the commercial enterprise was the one to find the——

Mr. WELLS. It could go either way. The NRC could find it or the licensee could find it, and it could both be noncited. Part of it has to do with NRC's regulatory philosophy that they are to provide oversight, not necessarily to be there on a day-in/day-out basis critiquing the operation of the nuclear power plant. There is a reliance on the operators to do a good job and fix things as they find them.

Mr. SHAYS. Right. Are they prevented if it's a noncited violation from verifying that it's been fixed?

Mr. WELLS. They are not prevented. If it happened to fall in their sample and they went out and looked and found that it was not corrected, I assume that there would be consequences to the licensee for not fixing it, or to the licensee who might have said, yeah, we did fix it, but they didn't.

Mr. SHAYS. Well, it seems to me, as you said, this classification tends to minimize the seriousness of the problem, which it certainly does. Non-cited violations do not require a written response from the licensee and do not require NRC inspectors to verify that the problem has been corrected.

Mr. WELLS. That's correct.

Mr. SHAYS. But it's really two parts. They don't even have to do a written response.

Mr. WELLS. No. That's correct.

Mr. SHAYS. I find that very surprising. I mean, really surprising. The NRC used non-cited violations extensively for serious problems, thereby allowing the licensee to correct the problem on their own without NRC verification of the correction.

So your point to us, which I think is serious, is that these are serious violations there also. And you stand by that?

Mr. WELLS. I do.

Mr. SHAYS. Consequently, NRC may not be fully aware of the quality of security at a site, and the lack of followup and verifica-

tion reduces assurances that needed improvements have been made.

I just would totally accept that as logical.

Let me just ask you, could someone find out how much time I have for the vote? Just check the TV.

That tells me that licensees are commercial enterprises,correct? And I have nothing against commercial enterprise. I happen to believe in it. That's one reason I am a Republican.

Mr. WELLS. That's correct.

Mr. SHAYS. But what I don't quite understand—am I to infer that they, in a sense, compete, that they view themselves as competitors and not sharing information? I mean, lessons learned is what I deeply care about. Are they sharing information with their competitors about screw-ups they have done in their own plants?

Mr. WELLS. That would be an excellent question to ask the industry folks that are on the third panel. We at GAO haven't done any specific work to look at sharing of information, but there is a lot of proprietary information out there. No question about it.

Mr. SHAYS. OK. Well, I believe you have done a helpful job. I sense that you are using your words in a measured way, which makes me think that we need to pay more attention to them than we may be. Is there anything you want to put on the record? Is there anything that we should have asked that we didn't that you wish we had asked?

Mr. WELLS. I think the continuing oversight by the Congress of the Nuclear Regulatory Agency is something that is important. They have a very important responsibility that's greatly increased since September 11, 2001, and I think the public deserves a lot more openness about where we are and what's happening. And I understand the security needs, but I also, you know, am sensitive to even as auditors going into an agency, a regulatory agency like the NRC, that sometimes I don't feel like we are getting as much cooperation in terms of trying to improve government operations as opposed to only trying to minimize how they answer our questions.

Mr. SHAYS. Yes.

Mr. WELLS. So I would hope that we and the future Commissioners of the NRC can work something out from an operating procedure because we are in this together to try to find out a better way to regulate a commercial nuclear industry that doesn't share a lot of concern about what may happen in the future from terrorist attacks. So we are there to help, and I am looking forward to that improved operation and working relationship.

Mr. SHAYS. Well, I think that you have earned that right to expect that.

Thank you.

Mr. WELLS. Thanks, Mr. Chairman.

Mr. SHAYS. That is a very measured report. I appreciate that.

I guess I am the chairman now for a second. I would just say to our first panel, you will be the first that we will call back as soon as we get back from voting. You really have about 20 minutes, if anybody wants to go downstairs and get something to eat. I think that it will probably have three more votes. I don't think we will keep you here that long. So I thank you all very much.

We stand in recess.

[Recess.]

Mr. SHAYS. We are back to order.

Both witnesses have been sworn in, and we sincerely appreciate you all waiting.

We do have some questions we would like to ask you based on the GAO's report. I would say to you that in my judgment, when you get into these issues of nuclear security and so on, you can really make things pretty sensationalized because the consequences can be quite significant. I view the GAO as someone who took no cheap shots, just came out with some concerns. I would like you to address them.

I need to have you explain to me, if you would, Mr. Reyes, why we are not seeing cited complaints and a written response to them as discussed in the report by the GAO.

Mr. REYES. The NRC requirements on violations, whether they are safety or security, is a graded approach.

Mr. SHAYS. Are what? I'm sorry.

Mr. REYES. Graded approach. In other words, for more significant violations, the licensee is required to provide an original response if appropriate.

For the noncited violations, which are the violations of lesser significance, we do not require them to send us a document. What we do require them is to put in their corrective action program. They have a program that is required by their quality assurance program to note any deviation or any violation of any requirement and to track the corrective action into full implementation.

Now, for significant violations, we do follow with NRC inspectors to confirm that all of those actions were taken and that they are effective. For the minor significant violations—we call them noncited violations—we do it on a sampling process.

Now, that doesn't mean that we don't know what's being done. See, I think there's a misconception that for those violations that we don't do a complete detailed followup we don't know what's been done. See, at every power plant in the country, the NRC has an office and has inspectors that live in the community and work there every day and interface with all of the employees at that station. So we do know, in general terms, what those that we didn't sample, the corrective actions were and what is being done. But we didn't send any specialist. We call them——

Mr. SHAYS. I should have known that, but you are saying you actually have someone onsite?

Mr. REYES. We have more—there are two NRC inspectors at each fuel—nuclear power plant and the field officers NRC——

Mr. SHAYS. I knew they were there. I didn't know they were specific onsite.

Mr. REYES [continuing]. Physically onsite on the facility. They live on the community. They have unfettered access to any part of the nuclear power plant.

Mr. SHAYS. So they don't have any operational responsibility. They can just walk wherever the hell they want.

Mr. REYES. Exactly right. At any time of day and night.

Mr. SHAYS. That sounds like an interesting job.

Mr. REYES. I used to be one when I earned an honest living, and I loved it.

Mr. SHAYS. It doesn't sound like an honest living.

Mr. REYES. It was. It was protecting public health and safety. But, at the same time, you have hands on and the real activity that was going on in a facility.

Mr. SHAYS. How do you avoid not developing such a personal relationship that you kind of close your eyes?

Mr. REYES. Very good question. We have a policy that we require them—first of all, there be two of. And the maximum time they can stay at one facility is 7 years, and we force them to rotate from one facility to another.

Then we have requirements from the supervisors from the regional offices to visit them at least quarterly to make sure there is—we call them objectivity reviews to make sure that in fact they are not being either unfair one way or the other. You can go either way.

Mr. SHAYS. OK. It is a strange terminology to call it minor significant violation, which is what you said. It sounds like you have three gradations here. But if it's significant, why is it minor? And if it is minor, why is it significant?

Mr. REYES. Maybe the terms are confusing. What we do, this panel that we referred to earlier, which is representative from all of the field offices and the headquarters program office, has guidelines in terms of the significance of the violation, and we—one of the categories, the lowest category, is called noncited violations, and I believe that's the one that GAO was referring to.

Mr. SHAYS. Right.

Mr. REYES. That we don't specifically follow through by sending inspectors to check every one of them. We do it in a sample approach.

Mr. SHAYS. Is someone who is falsifying papers, is that a significant violation?

Mr. REYES. I am going to have to defer——

Mr. SHAYS. Yes, talk to me a little bit about how you decide what is a cite, what isn't——

Mr. ZIMMERMAN. Good question.

Mr. SHAYS [continuing]. And who decides.

Mr. REYES. We decide.

Mr. ZIMMERMAN. It comes back to the panel that we talked about.

Mr. REYES. NRC panel.

Mr. ZIMMERMAN. NRC panel made up of representatives from each region and from our headquarters in Rockville. And what we look at, is it an isolated case or does it permeate the organization?

Mr. SHAYS. Right.

Mr. ZIMMERMAN. That's one of those factors that can help determine the significance of the item. How long has this been going on? Is this the first time it's been done? Or through our investigations—we have investigators. When we have a concern that potentially could be problematic in nature, we could use our investigators to come out and get additional information.

But the length of duration, what could have happened with the fact that this record of this door was not checked. If the door is alarmed and this was a belt and suspenders and the individual didn't check the door, but there is no reason to suspect the door all

of a sudden isn't working properly, does it work well afterward and before? And you check it afterwards, and it is still working, and it doesn't have a history of problems, a reasonable person could likely say that door probably would have worked, the belt and suspenders weren't there, but the door was still secure, as was the vital—those types of dialogs back and forth weighing the significance of this item is what this panel does.

A comment I didn't make in our earlier session of this is there was dialog that you had with GAO. Well, maybe this is a difference of opinion between what is a minor violation——

Mr. SHAYS. Right.

Mr. ZIMMERMAN [continuing]. And what significance is.

One of the things we are planning on looking at, because we have a review going on of what we call our significance determination process, which really is the hierarchy document, and we are piloting that activity right now. And it's possible—I don't know what the results will be, but it's possible that we may change some of our thoughts with regard to where that break point is between something being minor and something being more significant. That's an activity that we started in the July timeframe.

Mr. SHAYS. Let me yield such time as he may consume—not yield, let me give him the floor.

Mr. TIERNEY. Thank you, Mr. Chairman.

I would almost like to ask you a broad question. I would say that to the end I am still a little concerned with your force-on-force aspect and the finding that Wackenhut had knowledge that stand-by personnel had been used in test performances in the past. It seems that people were sort of trailing other people just to get the idea of where they might go and some of the information that would have been held inside and was not. Tell me why we shouldn't be concerned about that?

Mr. REYES. Let me give you the three major points; and then, if you need more details, I know Mr. Zimmerman has a lot of details.

But I think you need to remember, and I made that point earlier, DOE operates and regulates itself. In the case of the nuclear industry, commercial nuclear industry, we are the ones who do the oversight for those facilities. So when you bring the adversaries to do the force on force in this case you are talking about—is employees of this Wackenhut corporation. We, the NRC, review that in fact those individuals did the right thing. So we are the ones who are accepting their credentials and are they ready to do the test. We, the NRC, determine what the venue is that will be. And we are there in large numbers in the preparation and conduct of the test, and—as it is the NRC who decides whether the performance was acceptable or not.

Mr. TIERNEY. But still, apparently, someone still got the heads-up of how it was going to be done, what the attack would look like and be prepared for it.

Mr. REYES. But that is the Department of Energy example from the IG findings, and we are aware of those IG findings, and we have already trained our inspectors to look for those kinds of issues.

Mr. ZIMMERMAN. I think in the earlier session we talked about what we do every 3 years, where we will be with the adversary——

Mr. TIERNEY. Check that.

Mr. ZIMMERMAN. I will get back to you. Check the miles front and afterwards and all the things we do, the sensitivity we have toward it. Then we have the annual exercise that the licensee does, and I believe that we plan on observing those, but I want to make that distinction between those two different types.

The understanding that I have been given is at Y–12 it was not the DOE standard force on force where this occurred. It wasn't like our 3-year exercise. It was the off-year activity being done by the site, so that it had less oversight, less controls. It doesn't make it right, doesn't make it right. But I wanted to clarify for you that if in your mind you are looking at it and saying that equates to the NRC's 3-year force on force, I am trying to clarify that is not the——

[The information referred to follows:]

Insert 1 (for line 2362 of transcript)

Currently, all licensee employees with prior knowledge of the scenario are required to sign a form called Trusted Agent Responsibilities that, among other things, prohibits discussing the scenario with individuals who have not signed this form and who may participate in the exercise. To further limit dissemination of this information, the NRC strives to minimize the number of individuals who are asked to sign this form and, therefore, have access to scenario information. This form was reviewed and approved for use by the NRC's Office of the General Counsel. In addition, the NRC is developing a form that each member of the composite adversary force will sign, with similar prohibitions, and describing the responsibilities associated with the confidentiality of scenario information.

Mr. TIERNEY. I understand that. That we don't do those for every 3 years leads me to believe we ought to be concerned less about the annual periodic checks, that those don't occur either.

I am real concerned about these private enterprises policing themselves even if they aren't monitored by the NRC. It is like the fox watching the chicken coop here. I have a real problem with them doing the training and them deciding what the hours are going to be and them deciding what the force on force is going to be, even if they have your supervision——

Mr. ZIMMERMAN. They don't decide.

Mr. TIERNEY [continuing]. Your decisionmaking. There are examples of that information getting out and not being done right, and it is troublesome.

Mr. ZIMMERMAN. I understand the perception. They are not deciding anything. They are not deciding what path they are going to take. This is scripted by the NRC saying this is the path that you are going to take. The people doing it are our contractors.

Mr. TIERNEY. That's every 3 years.

Mr. ZIMMERMAN. Every 3 years.

Mr. TIERNEY. The annual ones—which I would imagine are just as important—that is not the case.

Mr. ZIMMERMAN. And the benefit of having a contract organization such as Wackenhut organization in place is that if I am one of the individuals who was selected to be on the composite adversary force I am going to learn an awful lot. Now I am going to take it back to my site and enhance the performance of those annual exercises, and I am going to bring back best practices associated with where I have been.

Mr. TIERNEY. I am not sure I buy that, Mr. Zimmerman. But, you know, I hear what you are saying, and I respect your opinion on that. But I am not sure I buy it.

Mr. ZIMMERMAN. Let me add one in closure——

Mr. TIERNEY. Sure.

Mr. ZIMMERMAN [continuing]. That will make you feel a little bit better. If it turns out the NRC is not satisfied with the performance of this group, we are going to do it ourselves. The Commission has told us that.

Mr. TIERNEY. But that is every 3 years.

Mr. REYES. He means the whole concept. The Commission is trying this approach right now. He is talking about the whole concept of Wackenhut supplying the adversaries. The Commission hasn't ruled out that we will have this—that this is the only way to go. We are doing this. The Commission can change their mind and say, no, we are going to do it differently.

Mr. ZIMMERMAN. The first use of this composite adversary force is occurring this week. This week is the first time it will be used in force on force. It will be on strength. If it doesn't meet our standards, then they will hear about it and the industry will hear about it. If there is the need for course corrections, they will be made.

Mr. TIERNEY. I have serious concerns on that. I would be interested if you would report to this committee what you find after that goes on and give us some detail on that.

Mr. ZIMMERMAN. I will do that.

[The information referred to follows:]

Insert 2 (for line 2434 of transcript)

The following are the findings from the first force-on-force exercise in which Wackenhut is used as the composite adversary force (CAF):

1. CAF members appear fit and conducted themselves in a military manner,
2. Leadership is knowledgeable, responsive, and articulate,
3. Members demonstrated basic operational planning and execution skills,
4. Tactical movements and use of cover and concealment were effective,
5. Weapons knowledge and employment were good,
6. CAF members conducted themselves in a professional manner at all times – unit cohesion is evident – they went to meals in formation,
7. There were some initial command and control issues within the CAF, which they seem to have resolved in later scenarios, and
8. CAF members interacted well with the NRC contractors.

Mr. TIERNEY. I would greatly appreciate that. That is one of the overriding concerns that I have, is that we are really not in charge of every aspect of who is in there providing security.

I don't want to use up too much of the time here.

Mr. SHAYS. I would just have a question—the gentleman yields the question.

Mr. TIERNEY. Now you have heard other people testifying here this morning. What do you think are the serious concerns that they raised and what is your response to those most serious concerns?

Mr. REYES. GAO audits are not complete, and they haven't visited the facilities. We are concerned that you are giving the impression that all they do is a paper review. We tried to bring some pictures.

Mr. TIERNEY. Correct me if I am wrong. You haven't visited all the facilities either?

Mr. SHAYS. I have to show you the pictures. The pictures to me were confusing.

Mr. REYES. OK. We cannot show you——

Mr. SHAYS. I don't understand why I should be impressed with someone who has a gun and a helmet on. Why would I feel good about this?

Mr. REYES. The physical barrier?

Mr. SHAYS. Yes.

Mr. REYES. See the physical barrier, the pop-up barrier?

Mr. SHAYS. Yes.

Mr. REYES. When GAO says that all that is going on is paper—we are trying to say there are physical changes at these facilities in the field. Now we couldn't bring pictures of everything.

Mr. SHAYS. OK. Tell me this——

Mr. TIERNEY. I think the concern was that you determined that those physical things were through a paper review in all but about four to six instances.

Mr. SHAYS. And, again, if the gentleman would yield just for a second. So this is the barrier.

Mr. ZIMMERMAN. A barrier.

Mr. REYES. Yes. A pop-up barrier.

Mr. ZIMMERMAN. It rolls down and pops up.

Mr. SHAYS. All right. I am not impressed.

Mr. REYES. But that is not a paper issue. I mean, there are physical barriers there.

Mr. SHAYS. What does this tell me?

Mr. REYES. You say that—bullet resistance.

Mr. ZIMMERMAN. Up. There you go.

Mr. REYES. That is a strategic point to show the adversary—I can't go into details but made out of bulletproof——

Mr. SHAYS. It is totally bulletproof.

Mr. REYES. Yes, sir.

Mr. SHAYS. That is helpful. I didn't know that.

Now this one.

Mr. ZIMMERMAN. Same thing.

Mr. REYES. Same thing. That is another strategic point. And we can't tell you how many officers.

Mr. SHAYS. What brings down something like this? It would have to be a grenade launch or a rocket?

Mr. REYES. You would have to have a sizable weapon.

Mr. SHAY. OK.

Mr. REYES. So our only point was trying to make that there are physical changes there. We couldn't bring you all the pictures. We really invite the committee or any of the staff on the committee to go and visit. Because in this forum we can't go into the details. But it's more than paper. We were surprised that they are characterizing it as that.

Mr. SHAYS. Is the gentleman also going to get into the issue, I hope?

Mr. TIERNEY. Just jump in.

Mr. SHAYS. No, I just wonder if you were going to pursue your questioning on the quality of the people.

Mr. TIERNEY. I don't know if you are going to bring that up or not. I am concerned and interested—I don't know whether I am the only one concerned about the quality of the people that are actually in there as security personnel. You know, the background check. Who is going the background check? How in depth it is. Who does their training? Who observes the performance on the job? Who determines whether or not they are properly proficient in weapons? Who determines that they are showing up on time, doctoring records, doing all those things?

Mr. REYES. The background checks are all done by the Feds. In other words, the FBI processes the fingerprints.

Mr. TIERNEY. So anytime Wackenhut or anybody else wants to hire somebody they have to check them through the FBI?

Mr. REYES. Yes, sir. Yes, sir. The psychological test is done by a contractor to the facility, but it's a doctor with his own credentials to go through that.

Now we are the ultimate who reviews that. Our inspection is called access controls. Contrary to what you heard here from GAO, we conduct those all the time and they are being conducted as we speak. So we are there where the rubber meets the road doing those inspections.

Mr. ZIMMERMAN. Background checks are more rigorous and more frequent than it is for other individuals that have vital area access because of the fact that these individuals are armed.

Mr. REYES. Yes, the armed individuals receive a more thorough review.

Mr. TIERNEY. Do you have any of the concerns raised by the Department of Energy or the GAO?

Mr. REYES. The recommendations, you mean?

Mr. TIERNEY. Yes.

Mr. REYES. We take them seriously. We have endorsed some of them. We have implemented some of them. Others we are still considering. We just haven't gotten to them and haven't ruled them out.

Mr. TIERNEY. Thank you.

Mr. SHAYS. Thank you.

I would just like to ask, and do this real quick because I want to get to the next panel, but I think you have been very responsive. I don't get a sense there are consequences if bad things happen. So make me feel good about consequences.

First off, anyone who was inebriate, drunk, they are fired, right?

Mr. REYES. Yes, sir.

Mr. SHAYS. OK. And then there is the question as to how that would have happened. So you don't want a written explanation from—why wouldn't there be at least a written explanation?

Mr. REYES. There is an aside. We know that the individual was fired. Typically, it was by the supervisor observation program. The supervisors of these individuals are trained to observe behavior. So the way it is found out is typically we have a report that a supervisor requests it for cause, testing of an individual.

We know an individual is no longer aware, and we are aware of the corrective actions we are taking over all of the facility. We may not send an inspector just to review that in detail. Our inspectors onsite are aware that this individual is not coming back, and they are in discussion with the other security guards, and that's why we have the inspector at the plant who has access to all 1,000 employees. They know and they ask, do you know what happened, and make sure that word gets out that is not tolerated. We do have indirect means to confirming it. I think there is a misnomer on——

Mr. SHAYS. Wait. If you have people onsite, it seems to me you are able to check it the next day. That's why I am beginning to think, if you have people onsite, they are aware of the citations, correct?

Mr. REYES. Yes.

Mr. SHAYS. Don't they write you a note and say this has been corrected?

Mr. REYES. If we go and follow it, they do. But we have a very prescribed inspection program that includes safety and security. And we want them to go in the control room and we want them to check the safety pumps. It is just a matter of make sure you are putting your resources where the highest safety and significance matter is.

Mr. SHAYS. I would think that the people onsite would be asked to verify any citation, every criticism in the plant. I would think that's what they need to do. And I would think they need to write a report on everyone. I mean, it just seems like a no-brainer. They are there.

Mr. REYES. They are busy. And they write a report. And the most significant ones, they are aware of the other ones.

Mr. SHAYS. How difficult is it to followup on a complaint and check it out? They could do it in an hour or two, couldn't they?

Mr. REYES. Well, it typically takes more than that.

Mr. SHAYS. Better they do it than no one do it.

Mr. REYES. But we do it, sir, on a sample basis. We do.

Mr. SHAYS. I am going to have that explained to me later. I am impressed you have people onsite. I am not impressed that they are not following up on cited complaints or noncited complaints.

Anything else you want to put on the record that you would like to—yes.

Mr. ZIMMERMAN. I just want to make a comment—I guess maybe two comments, maybe one on legislation. But the comment I want to make is that I got the sense from reviewing the hearing from last year and from sitting here today that a number of the members of the committee have a concern that we don't worry enough, that we are complacent, why aren't we laying awake at night?

And I want to tell you that we are laying awake at night, that we are very concerned, that this agency is about continuous improvement and that we are constantly looking and working very long hours in an effort to get out in front of those that mean to do us harm.

So there's a very—I am very proud of the staff at the NRC, and we are very much focused, again, on trying to search for continuous improvement, and we are not lackadaisical. We are—I am not saying that we are, but, again——

Mr. SHAYS. I think you have judged us fairly well in terms of our concern.

I have a feeling that the way we set up DOE, we have those who promote and those who are looking to be the inspectors and to do security. And I feel for some reason we still don't have that separation with NRC. I don't know why we don't.

Mr. ZIMMERMAN. That's why I am raising it. I am trying to, in words at least, say it—and then through everything that we have tried to do in our explanation. Because we are not sure that our issues have stuck.

Mr. SHAYS. I think you are going to have a hard time convincing us in that area. By setting up a separate organization, there will be some natural tensions that I don't think exist within the NRC, and so I think you are going to have some real skepticism on our part about that. And so I understand that you have divided responsibilities. That's the challenge.

Mr. REYES. I just want to thank the committee for inviting us here. We are looking forward to coming back and keeping you updated on the action we are taking. We do want to ask your support on the legislative request that we have in front of Congress. It is of the most importance, that those laws are passed so we can protect our nuclear power plants better.

Thank you very much.

Mr. SHAYS. Hold on 1 second. OK. I want to put it on the record. I would like you to just ask this question or make this point and have you react to it.

Mr. HALLORAN. This is the point that I think you made before, in terms of the zeal of the regulatory effort. DOE is an operator of sites, NRC is a regulator, so you are necessarily one step removed from turning the knobs and——

Mr. REYES. We are.

Mr. HALLORAN [continuing]. And putting up the fences. So that dictates some different operational structures and ways to get things done, doesn't necessarily demand a lesser intensity level, but I think it does require a different approach.

Mr. SHAYS. See, I think he gave a better answer than you did. He made a better defense of your case, I think. I wanted to put it on the record. I am making an assumption. I made a parallel in which I am being challenged, and that is that the parallel isn't the same—that you are a regular. I guess, I also view you as promoters of the industry. I do feel that way. So, at any rate——

Anything else to put on the record?

Mr. REYES. No. We want to reinforce the legislative request that we have then. We really need those legislative enhancements.

Thank you very much.

Mr. SHAYS. Don't be offended I said he did a better job. He is a really bright guy.

Mr. REYES. No, we are not.

Mr. SHAYS. Thank you for waiting, and I appreciate your willingness to fit into our needs. Thank you very much.

Mr. REYES. Thank you.

Mr. SHAYS. I will call on our last panel—thank you for being here.

Mr. Alex Matthiessen, director, Hudson Riverkeeper, Garrison, NY; Mr. David Lochbaum, the Union of Concerned Scientists, based in Washington, DC; and Mr. Marvin Fertel, vice president and chief nuclear officer at Nuclear Energy Institute.

With that, if you would—thank you for standing.

[Witnesses sworn.]

Mr. SHAYS. I would note for the record our witnesses responded in the affirmative.

Mr. Fertel, you were a dead giveaway in the audience because any time the Commission made a comment that you liked you smiled broadly, and I thought—you would not be a good poker player, sir.

Mr. FERTEL. I am just too straight.

Mr. SHAYS. OK. Well, that's a good answer.

All right. Mr. Matthiessen, we will start with you; and we will just go right down the line. Thank you very much.

Mr. MATTHIESSEN. Terrific.

Mr. SHAYS. Nice to have you all here.

STATEMENTS OF ALEX MATTHIESSEN, DIRECTOR, HUDSON RIVERKEEPER, GARRISON, NY; DAVID LOCHBAUM, UNION OF CONCERNED SCIENTISTS, WASHINGTON, DC; AND MARVIN FERTEL, VICE PRESIDENT AND CHIEF NUCLEAR OFFICER, NUCLEAR ENERGY INSTITUTE, WASHINGTON, DC

Mr. MATTHIESSEN. Thank you for having me, Chairman Shays, members of the subcommittee. Thank you for the opportunity to once again testify on safety and security at Indian Point; and thank you, Congressman Shays, for your leadership to date on this issue.

I also want to say I was very encouraged by the line of questioning, questions that we heard from members of the subcommittee today.

Riverkeeper is not and has never been an anti-nuclear organization. Our campaign aims only to minimize the risks associated with the Indian Point nuclear facility and by necessity aid in the reform of those Federal and State agencies and policies governing the plant.

Three years after September 11, Indian Point still is unprepared to repel an attack from the air, land or water or a combination thereof. While improvements have been made at the margins, there remain gaping holes in Indian Point security. On the ground, current guards tell us that in some areas security at the plant is worse than it was before September 11, 2001. The spent fuel pools remain largely unprotected.

Mr. SHAYS. Let me just say something to you. When you make a comment like that, this is a comment that you are saying under oath. So this is not casual comments, correct?

Mr. MATTHIESSEN. No.

OK. This is based on conversations that I have had with a current security guard at the plant, and he is relaying, in turn, comments that he has gotten from other guards.

Many of the best-trained and most-experienced guards have been fired or have quit. This is according to the guard's report that we have heard only a week and a half or 2 weeks ago—morale is low, and guards say they feel no obligation to stay on their posts in event of an attack. A chilled environment exists at the plant, and Entergy management is apparently still telling security personnel to alter incident reports.

There are no specific defenses against an aerial attack at Indian Point—no no-fly zone, no combat patrols, no anti- aircraft missiles, nothing.

From the water, there is no physical barrier to prevent a tanker or a speedboat loaded with explosives from plowing into the cooling water intakes.

With regard to the NRC's force-on-force security drills, they are a joke—but not a funny one. The NRC drills are designed to allow nuclear systems to game the system. Everyone knows that if real conditions were used and no limits put on well-trained mock attackers, the plans would fail nearly every time.

Again, I have details reported by POGO and other groups as well as the guards themselves.

A head-in-the-sand mindset has a fever grip on the NRC and FEMA, which has refused to accept the new threat level and revamp organizations accordingly. The NRC and FEMA are captive to the industry they regulate, and the Department of Homeland Security has failed to assert itself. As a result, these agencies have little credibility with the American people, which in turn undermines public safety.

Allow me to identify just three of many problems plaguing the NRC:

First, the NRC resists the need to consider terrorism in administrative proceedings, and yet they routinely invoke terrorism to justify a new wave of policies designed to thwart the public's right and need to scrutinize the industry.

Second, the NRC's new design base threat level is set too low. David Lochbaum will cover this in detail, but allow me to add that there remains a considerable gap between the level of defense plant operators are expected to provide and what the U.S. military is prepared to deploy.

Finally, the NRC continues to enact policies that allow it and the nuclear industry to operate in increasing secrecy and with reduced transparency and public participation. I assure you—and I know you know this—that the less the public is able to see the more dangerous this industry will become.

Now moving into recommendations. The best way to truly minimize the public health and safety risks at Indian Point is to close the plant and secure the onsite spent fuel. However, so long as Indian Point is still operating, there are numerous ways to better protect the plant. I will highlight those three or four measures that I think are the most urgent and readily achievable.

First, we must secure the plant against aerial or waterborne attacks, which we can do with relatively inexpensive passive technologies. Installing a Beamhenge system, a line of steel beams set vertically in deep concrete foundations connected by a web of high-strength cables, wires and netting, would effectively shield the facility's vital components and structures. Beamhenge is essentially the nuclear grade equivalent of the fences erected around golf driving ranges. Dunlop barriers, inflated cylinders of rubber-coated textile linked together or anchored to a mooring buoy, should be installed in the Hudson River in front of Indian Point to help protect the plant's cooling water structures. Already in place at several Navy bases, Dunlop barriers are used to thwart small boat terrorist attacks.

Second, we must establish a temporary no-fly zone over Indian Point, combined with combat air patrols, at least until the passive defense systems are in place.

Third, Congress must direct the NRC to deal more aggressively with the highly vulnerable spent fuel stored at nuclear reactor sites. The best way to do that is to install hardened onsite storage systems, or HOSS, which is designed to contain isolated radiation and repel terrorist attacks.

Finally, Congress must direct the NRC and FEMA to revamp their policies and regulations governing nuclear plant security and emergency preparedness.

I have a whole laundry list of specifics there, but I will wait until the Q&A—if I have the opportunity to list those—in the interest of time.

In general, though, I think it would be good for Congress to consider appointing a task force made up of governmental and non-governmental stakeholders to do a top-to-bottom review of the NRC and FEMA's oversight of this industry.

In conclusion, little has changed since September 11 regarding the level of security at Indian Point. Federal agencies remain in a state of denial regarding the security threat facing nuclear facilities. Congress needs to ask the NRC and the industry—and I am paraphrasing the gentleman who was from the NRC who was here just a minute ago—if you are so concerned and laying awake at night, why aren't you concerned about deploying the most obvious and inexpensive security measures at our most vulnerable and high-risk nuclear plants?

Whether they admit it or not, I believe the answer is quite simple. The industry and the NRC don't want to draw public attention to the intrinsic danger of nuclear power and the naked vulnerability of these facilities to terrorist attack, especially at a time when the industry is hoping to build a whole new generation of nuclear energy plants.

The Federal Government's current approach to nuclear plant security and emergency preparedness is leading us down a path that could—God forbid—result in a far more terrifying attack than what we experienced that horrible day 3 years ago. We have received the warning signs regarding the possibility of and our vulnerability to a terrorist attack on a U.S. nuclear power plant, much as the government had received warnings about the September 11 attacks. Let's not give a future 9/11 Commission the opportunity to say we

knew a nuclear attack on a power plant was possible and we did too little to stop it or to minimize the impacts.

Thank you very much for giving me the opportunity to share my views today.

Mr. SHAYS. Thank you, Mr. Matthiessen.

[The prepared statement of Mr. Matthiessen follows:]

TESTIMONY OF ALEX MATTHIESSEN

Executive Director, Riverkeeper, Inc.

U.S. Congressional Subcommittee Hearing on *Emerging Threats: Assessing Public Safety and Security Measures at Nuclear Power Facilities*

Rep. Christopher Shays, Connecticut
Subcommittee Chairman

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

Scheduled for Tuesday, September 14, 2004

Room 2247 Rayburn House Office Building.

Washington, DC

****

Subcommittee Chairman Christopher H. Shays and members of the subcommittee:

Thank you for the opportunity to once again provide testimony on this crucial public health and safety issue affecting millions of people living and working in the populated region surrounding the Indian Point nuclear power plant.

I am Alex Matthiessen, executive director for Riverkeeper, Inc, an independent, member-supported, not-for-profit organization whose mission is to protect the Hudson River and to safeguard the New York City drinking water supply that serves over 9 million New Yorkers. Since its founding in 1966, Riverkeeper has led the battle to restore the Hudson River and has successfully prosecuted hundreds of environmental law breakers. Riverkeeper and its predecessor, the Hudson River Fishermen's Association, Inc., has nearly 40 years of experience with Hudson River issues, and is a leader in the pursuit of economically viable and ecologically sound power plants.

Riverkeeper is not and has never been an anti-nuclear organization. Our focus is solely on the Indian Point nuclear power plant and the federal policies that affect Indian Point and the communities surrounding the facility.

I. BACKGROUND

A. Unique Characteristics

The Indian Point nuclear power plant, located in Buchanan, NY, on the Hudson River, 35 miles north of Times Square in New York City, is situated in the midst of the densest population surrounding any U.S. commercial reactor site in the country. Over 300,000 people live within a 10-mile radius of Indian Point and nearly twenty million people live within a 50-mile radius.

Indian Point is in close proximity to the nation's financial and media center and transportation hub. It looms over the nation's largest regional metropolitan economy, which is home to numerous Fortune 500 companies.

Indian Point is just miles from the Croton, West Branch and Kensico reservoirs which provide drinking water for 9 million Westchester County and New York City residents.

These are just a few of the reasons why our organization, along with 70 others, has argued that Indian Point is a unique case that deserves special attention from the federal government. Given al Qaeda's apparent fixation on New York and the group's stated aim of using a future attack to maximize economic and psychological damage and loss of life, Indian Point is arguably one of the most attractive terrorist targets in the country.

In 1979, in the wake of the Three Mile Island meltdown, NRC's Director of the Office of State Programs, Robert Ryan stated that:

> "...it is insane to have a three-unit reactor on the Hudson River in Westchester County, 40 miles from Time Square, 20 miles from the Bronx. And if you

> describe that 50-mile circle, as I said before, you've got 21 million people. And that's crazy. I'm sorry. I just don't think that that's the right place to put a nuclear facility."

If, decades ago, doubt existed regarding Indian Point's location, then post September 11th we really need to question the wisdom of allowing Indian Point to continue operating in close proximity to such a densely populated area. Clearly, today, we would not site Indian Point this close to the New York City metropolitan area.

Prompted by concerns regarding security, emergency preparedness and safety, over 400 elected officials at the local, state, and federal level are calling for Indian Point's shutdown. At the local level, over 50 municipalities have passed resolutions calling for an end to the plant's operation.

B. 9/11 Commission Report Reveals That the Threat to Indian Point is Real

The 9/11 Commission Report, released in late July, revealed that Mohamed Atta, the plot's ringleader, who piloted one of the planes that hit the World Trade Center, "considered targeting a nuclear facility he had seen during familiarization flights near New York."

While the nuclear plant was not identified in the report, several strong pieces of evidence suggest Indian Point. First, the terrorists had rented planes from Teterboro Airport – in northern New Jersey about 30 miles from Indian Point – for their reconnaissance flights. Second, the terrorists' test flights included trips along the Hudson River corridor which the terrorists used as a guide on their way to the World Trade Towers on 9/11. Third, Indian Point is the only nuclear power plant in the Hudson corridor. Among other area nuclear plants, Indian Point is the closest to New York City.

A June 16, 2004 9/11 Commission Staff statement reinforces earlier reports that the original plot for September 11th was to involve attacks on nuclear power plants. According to the statement: "K.S.M. [Khalid Sheikh Mohammed] maintains that his initial proposal involved hijacking 10 planes to attack targets on both the East and West Coasts of the United States...[including] C.I.A. and F.B.I. headquarters, unidentified nuclear power plants and the tallest buildings in California and Washington State." [emphasis added]

In startling testimony before the 9/11 commission on June 16, two CIA officials claimed the agency has thwarted several al-Qaeda attacks since Sept. 11, 2001, and one said, *"I think we've probably prevented a few aviation attacks against both the East and West coasts."* A nuclear power plant, possibly Indian Point, could have been a target of these thwarted attacks.

If Indian Point was among the "unidentified nuclear power plants" targeted in the original plot, then our federal government must assume that terrorists may attack Indian Point in the future. Let's not forget that before the terrorists brought down the World Trade Towers on September 11, 2001 the WTC site had been targeted before – back in February 1993.

C. Gaps and Weaknesses in Emergency Preparedness and Security

Emergency Planning

Since the attacks of September 11th, legitimate concerns have been brought up by members of the public and elected officials regarding the inability of the emergency preparedness plan to protect the public in the event of a radioactive release from Indian Point. Valid concerns have also been raised about security lapses and poor security defenses at Indian Point. These issues are closely entwined.

Concerns about deficiencies within the plant's emergency plan were validated by the March 2003 release of the final report by James Lee Witt Associates on the adequacy of Indian Point's emergency plan. The report's conclusions are decisive, irrefutable and inescapable. With regard to the "problems" associated with the emergency plan, Witt Associates states that,

> "...it is our conclusion that the current radiological response system and capabilities are not adequate to overcome their combined weight and protect the people from an unacceptable dose of radiation in the event of a release from Indian Point."

The Witt report, commissioned by New York State Governor Pataki, went on to say that "this is especially true if the release is faster or larger than the typical exercise scenario." This is a key point given the fact that the latest biennial emergency exercise conducted for Indian Point back in early June did not involve a fast breaking release of radiation. In fact, it failed to incorporate a simulated release of radiation altogether!

The June exercise spearheaded by DHS, FEMA and the NRC was highly orchestrated and geared mostly towards public relations than public safety. While June 8, 2004 will go into the history books as the first time federal agencies held a radiological emergency exercise for a nuclear power plant featuring a mock terrorist scenario, it will be remembered for exhibiting our federal government at its very worst.

At the heart of the exercise scenario, a hijacked 767 commercial airplane crashed into a parking lot and careened into a transformer on the Indian Point site. With the transformer knocked out, and the subsequent loss of offsite power, a chain of events unfolded that culminated with the threat of a reactor core meltdown. The scenario evolved over a ten hour period and resulted in no releases. This left many scratching their heads since last summer the NRC and FEMA told the press that the next exercise would involve a fast-breaking release of radiation.

Most troubling were statements made to the press by NRC officials which were clearly designed to imply that the 767 crashed into a containment dome but failed to penetrate and cause a release. In one instance Brian Holian, deputy director of reactor projects for NRC Region I, was quoted in the press as saying "[the] scenario of the crash included no damage to the reactor's concrete containment building" and then in the same breath stated that recent studies showed "most plane crashes into containment buildings would not result in significant releases of radiation."

Holian's comments are an obvious ploy indicative of a broader public relations effort on the part of the Department of Homeland Security, FEMA, NRC and Entergy designed to convince the public that Indian Point is not vulnerable to a terrorist attack.

In fact, determined terrorists targeting Indian Point could succeed in breaching a reactor containment dome and damaging the reactor core, resulting in a subsequent release of radiation. A successful terrorist strike on one of the spent fuel pools could result in a pool fire and major radioactive release.

What remains so disturbing is how these agencies have been able to certify Indian Point's unworkable emergency plan while providing so little evidence that the plan would actually protect the public.

Plant Security

On the matter of security, Indian Point continues to lack appropriate defense systems to repel an attack from the air, land and water. The spent fuel pools, cooling intakes, steam lines, control room buildings, transmission lines and back-up diesel generators remain vulnerable targets. In section III we present recommendations for boosting security at the plant in a manner that will better protect these vulnerable targets.

It is also important to note that security officers at Indian Point continue to raise concerns about poor training and weak testing. Last September, the Project on Government Oversight (POGO) criticized the NRC for making the July 2003 force-on-force security exercise at Indian Point too easy. POGO's criticisms were based on information gathered from participants and observers of the test. Among the major problems identified:

- The number of attackers in the test was "barely above the much-ridiculed" three attackers required under pre-9/11 security rules, POGO pointed out that "the intelligence community generally believes that terrorists would attack a target with a squad-sized force, which in the Army is 12 and the Navy is 14";

- The attack simulation did not incorporate the possible use by terrorists of commonly available weaponry including .50 caliber rifles with armor-piercing incendiary rounds, or rocket-propelled grenades;

- All three force-on-force tests took place in broad daylight although intelligence experts agree that an attack would likely take place in the dark. In two drills "mock terrorists crossed open fields in broad daylight in order to reach the protected area, making it that much easier for them to be observed by the security officers"; and

- Mock terrorists were security officers from another plant who had no training in terrorist tactics.

NRC officials claim the role of security officers is to hold off attackers until outside responders arrive. However, as POGO correctly notes, tests have shown that an attack is generally won or

lost in between three and eight minutes, and SWAT response times are proven to be between one and two hours.

Also disturbing is that documents leaked to POGO in the spring of 2003 revealed that Indian Point's owner crammed for the July test. POGO's investigations found that with months of advance notice from the NRC, nuclear plants often game the testing system, hiring security consultants and additional guards in the months leading up to the force-on-force tests. Once the tests are completed, security consultants are let go and the guard force reduced until the next test. The July 2003 exercise for Indian Point exemplifies POGO's findings.

Many of these issues were also discussed in an internal January 2002 Entergy report that was leaked to Riverkeeper in December 2002. The January 2002 report, which was best know for documenting that only 19 percent of the guard force believed they could successfully defend the plant against a terrorist attack, infuriated local, state, and federal officials because it directly contradicted past proclamations – issued by Entergy, the U.S. Nuclear Regulatory Commission, and the State Office of Public Security – that Indian Point is secure. One can only wonder what Mr. Kallstrom was thinking about on Dec. 13, 2001 when he declared Indian Point to be the best defended facility in the nation and brazenly taunted terrorists to attempt an assault on the plant. His statement, troubling then, is more disturbing now given that very the next month a security consultant for Entergy delivered his report.

D. Catastrophic Consequences

The bottom line for this public health and safety issue is that the risks associated with Indian Point far outweigh the benefits. There is no question that the risks are significant and the consequences catastrophic.

A new study released by Riverkeeper on September 8 found that the potential health consequences of a successful terrorist attack on the Indian Point nuclear plant could exceed 500,000 long-term cancer fatalities and reach 44,000 early fatalities under worst-case conditions. Dr. Edwin Lyman, a senior staff scientist in the Global Security Program at the Union of Concerned Scientists, authored the report titled "Chernobyl-on-the-Hudson?: The Health and Economic Impacts of a Terrorist Attack at the Indian Point Nuclear Plant."

The study uses the NRC's current computer models and methodology to update a 1982 congressional report based on Sandia National Laboratories' CRAC-2 (Calculation of Reactor Accident Consequences) study. CRAC-2 found that a core meltdown and consequent radiological release at one of the two operating Indian Point reactors could cause 50,000 early fatalities from acute radiation syndrome and 14,000 latent fatalities from cancer.

Given a successful attack at one of the two operating Indian Point reactors, the report finds that:

- The number of near-term deaths within 50 miles, due to lethal radiation exposures received within 7 days after the attack, is approximately 3,500 for 95th percentile weather conditions, and approximately 44,000 for the worst case evaluated. Although the report assumed that the 10-mile emergency planning zone was entirely evacuated in these cases,

this effort was inadequate because (according to Entergy's own estimate) it would take nearly 9.5 hours to fully evacuate the 10-mile zone, whereas in the report's model the first radiological release occurs about two hours after the attack.

- Near-term deaths can occur among individuals living as far as 18 miles from Indian Point for the 95th percentile case, and as far as 60 miles away in the worst case evaluated. Timely sheltering could be effective in reducing the number of near-term deaths among people residing outside of the 10-mile emergency planning zone, but currently no formal emergency plan is required for these individuals.

- The number of long-term cancer deaths within 50 miles, due to non-acutely lethal radiation exposures within 7 days after the attack, is almost 100,000 for 95th percentile weather conditions and more than 500,000 for the worst weather case evaluated. The peak value corresponds to an attack timed to coincide with weather conditions that maximize radioactive fallout over New York City.

- Based on the 95th percentile case, Food and Drug Administration guidance would recommend that many New York City residents under 40, and children in particular, take potassium iodide (KI) to block absorption for radioactive iodine in the thyroid. However, there is no requirement that KI be stockpiled for use in New York City.

- The economic damages within 100 miles would exceed $1.1 trillion for the 95th percentile case, and could be as great as $2.1 trillion for the worst case evaluated, based on Environmental Protection Agency guidance for population relocation and cleanup.

The report's executive summary is included as Attachment A to this testimony. The full report is available at www.riverkeeper.org.

Finally, as we presented in our written testimony to this subcommittee in March 2002, the NRC's own documents reveal that the consequences of a large release could be severe. We touched upon several of these documents in testimony we provided in March of last year to this subcommittee.

II. THE FEDERAL GOVERNMENT'S APPROACH TO NUCLEAR SECURITY AND EMERGENCY PREPAREDNESS

For the federal agencies that regulate the nuclear power industry, corporate profits continue to be placed above public safety. The NRC and FEMA/DHS clearly have fallen captive to the industry they regulate. In addition, a bureaucratic paralysis or head-in-the-sand mindset appears to be plaguing the NRC and FEMA/DHS. These agencies seem unwilling to accept the new threat level and revamp regulations accordingly. As a result these agencies lack credibility with the American public which ultimately undermines their ability to effectively fulfill their responsibilities.

There are a number of major problems with the manner in which the federal government is currently handling security and emergency preparedness. Below, we touch upon just six of these.

A. NRC Refuses To Consider Terrorism In Administrative Proceedings

The NRC has ruled, in several recent administrative proceedings, that since terrorism is too speculative under the NEPA (National Environmental Policy Act) process, the issue of terrorism cannot be raised in site-specific proceedings such as license renewal. The NRC has argued that since the probability of terrorism cannot be estimated that it is not a matter that it needs to address within administrative proceedings. Ironically, the NRC consistently uses the threat of terrorism to justify their new policies that reduce the opportunities for public participation.

B. Design Basis Threat Level Is Set Too Low

The NRC has set its new post-9/11 Design Basis Threat (DBT) level too low. The DBT, which defines the size and capability of potential attackers that nuclear power plant owners must protect against, has been set at a level far short of the actual threat level we face today, even after the NRC's recent DBT upgrade. Force-on-force exercises likewise ought to be based on defending against a much a larger threat than the current DBT.

Another issue pertaining to the DBT relates to the federal government's role in protecting nuclear power plants against any threat above the DBT. Since plant operators are not required to defend against the threat above the DBT, is the federal government prepared to? Past news coverage has revealed that there is confusion among the federal agencies as to who is responsible for what and which agency would take authority in event of an attack on a nuclear power plant. Furthermore, while plant operators are tested in accordance with the DBT it remains unclear whether the federal government, for example the Department of Defense, is tested for its ability to prevent an attack that is above and beyond the DBT threshold.

C. Force-On-Force Exercises Are Highly Staged

The NRC's July 2003 force-on-force exercise at Indian Point lacked any element of surprise and as a result it failed to serve as evidence that the plant's security force could effectively repel an attack. This force-on-force exercise is explained in more detail earlier in the testimony.

D. Emergency Preparedness Regulations Are Inadequate

NRC and FEMA emergency preparedness regulations fail to take into consideration the unique conditions associated with a terrorist attack on a nuclear power plant and the implications for emergency response. The current emergency plan fails to address:

- A scenario involving a fast breaking release of radiation that results in significant contamination.

- A scenario in which the radioactive release contaminates a significant portion of the 10-mile emergency planning zone and parts of the 50-mile ingestion pathway zone and exposes citizens to higher-than-acceptable doses.
- A scenario involving major transportation arteries that are rendered impassable (either by acts of terrorism or gridlock) to people evacuating.
- A scenario in which a large number of people, who have been injured and contaminated and require treatment and decontamination.

E. Plant Licenses Are Not Required To Defend Against "Enemies of the U.S."

NRC regulations[1] do not require nuclear plant licensees from having to protect their facilities from a military attack by a foreign power, but rather a sub-national terrorist group. The "enemy of the United States" provision, 10 CFR §50.13, exempts licensees, like Entergy, from providing "design features or other measures for ... protection against the effects of attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person." While the NRC licensees are responsible for protecting nuclear plants from sub-national groups, and the military is responsible for protecting them from attacks by the armed forces of enemies of the United States, the regulations are silent as to who is responsible for the range of threats in between these extremes. As a result, it is not immediately obvious where al Qaeda and other terrorist organizations fall in this classification.

The NRC has refused to consider implementing measures to protect nuclear plants from 9/11-type airborne assaults, claiming that it is the responsibility of the Federal government, and not nuclear plant owners, to protect against "enemies of the United States." This gap in security leaves Indian Point dangerously vulnerable. Yet without an entity that has the authority to develop an adequate standard of protection for this plant, there is little hope that this security gap will be closed any time soon.

F. NRC Shrouded in Secrecy

The NRC continues to enact policies that allow it – and the nuclear industry it regulates – to operate in increasing secrecy and with reduced transparency and public participation. This will further undermine plant security and jeopardize public health and safety. Given the NRC's track record of poor oversight, public scrutiny is needed more than ever.

Riverkeeper criticized the U.S. Nuclear Regulatory Commission's August 4, 2004 declaration that the agency will no longer make available to the public the results of physical assessments of nuclear plant security or enforcement actions associated with such evaluations. Until now, the

[1] According to NRC regulations (10 CFR §73.55), NRC-licensed nuclear power plants must be provided with physical protection systems designed to protect against the design basis threat (DBT). The DBT is a description of the characteristics of an adversary force seeking to cause a radiological sabotage event (or theft or diversion of special nuclear materials from Category I fuel cycle facilities). Until recently, the DBT conformed to a set of very general, rather weak requirements (10 CFR §73.1), the majority of which were formulated in the late 1970s, based on what was believed to constitute a credible terrorist threat at the time. The DBT is meant to characterize the threat posed by a subnational terrorist group.

NRC has provided regular public updates on vulnerabilities and lapses that NRC inspectors have discovered at the country's 103 nuclear power reactors, such as weaknesses in training programs.

Lengthy discussions preceded the NRC's decision four years ago to put plant performance evaluations on the agency's Web site. Immediately after 9/11, the NRC pulled almost all information from its Web site and carefully vetted thousands of documents. The information was reviewed and, in many cases, put back on the site after being deemed acceptable for public consumption. The NRC's move to remove performance evaluations from their website, has left many asking "Why the sudden policy reversal?"

The NRC's policy change raises the question of whether the real intent is to shield plant owners from embarrassing security blunders becoming public. Last September, following the release of a report from the Government Accountability Office on nuclear plant security, the *New York Times* revealed that the NRC security assessment – which discovered a security officer asleep while on duty – occurred at Indian Point. NRC inspectors treated the Indian Point incident as a "non-cited violation because it did not affect plant security, according to a report issued by the commission that describes an inspection at the plant. The NRC's report also says the commission did not treat the incident more seriously because no guards had been found sleeping "more than twice during the past year." The GAO report noted that nationwide, the NRC tended not to issue formal citations and to minimize the significance of problems it found if the problems did not cause actual damage. In other words, since a terrorist attack did not take place while the security officer was asleep, the NRC refused to cite the plant's owner in violation of standards.

Ultimately, the NRC's new policy undermines security and makes Indian Point a more attractive terrorist target. Absent an explanation of what substantial security improvements have been made, one can only assume that little has been done to protect plants like Indian Point. The NRC is fooling no one – certainly not the people of New York and surely not the terrorists determined to strike again.

In addition, the NRC's new policy will further erode public confidence in the Commission's performance and calls into question whether the Commission is taking the appropriate actions to ensure that nuclear plants like Indian Point are not vulnerable to terrorist attack.

Security is a key component of the NRC's Reactor Oversight Process for Indian Point and other plants. Removing security from public scrutiny erodes much-needed transparency. Security concerns should be acknowledged and resolved, rather than shielded from the public. As a result, security gaffes will no longer be subject to the kind of public scrutiny that forces change.

III. RECOMMENDATIONS FOR IMPROVING SECURITY

The best way to truly minimize the public health and safety risks is to close the plant and secure the on-site spent fuel. **Section A** addresses the reduced risk associated with plant closure. Prior to the plant closing, and for a period after closure, strong security is crucial. **Section B** provides a series of recommendations for strengthening security at Indian Point.

A. Once Closed, Indian Point Becomes Less Of A Threat To Public Health And Safety

Closing Indian Point would have an immediate benefit. Just 20 days after shutdown, the radioactive inventory within the reactor containment buildings will decrease significantly through half-life decay. Consequent reductions in early fatalities within the 10-mile radius emergency planning zone would be 80%. Within the 50-mile radius ingestion pathway zone, there would be a 50% reduction in latent cancer fatalities. Given the high population density around the plant these percentages translate into tens of thousands of saved lives in the event of a catastrophic release triggered by accident or terrorist attack.

In addition, removing the fuel from the reactors – something that can be done approximately a week after shutdown – will allow security forces to focus their protection on the deadly irradiated fuel stored in the pools.

Moreover, a plant that is closed is no longer producing the irradiated fuel rods, which are most dangerous in the first six months upon removal from the reactor core.

It is easier to protect and monitor a reactor that is shut down. The site is most vulnerable while the reactor is operating. There are a number of ways to cause a meltdown of the reactor: cutting off-site power, destroying the cooling water intakes, sabotage/destruction of safety systems, destruction of the control room, as well as crashing a jet into the reactor building. The propensity of a reactor core to melt, if the flow of cooling water to the core is interrupted, is substantially reduced within just a few hours of shutdown.

B. Upgrading Indian Point's Security

1) Harden Spent Fuel Storage Systems: Indian Point's irradiated ("spent") fuel[2] stockpile must be better safeguarded. The current pool storage system and the proposed dry storage cask installation are grossly inadequate to protect public and worker health and safety. We propose instead the HOSS[3] system, designed to contain and isolate radiation and repel terrorist attacks. HOSS can substantially diminish the risks associated with irradiated waste fuel storage by separating it into small batches, thereby eliminating the danger of one of the worst possible nuclear disasters – a fuel pool fire. HOSS is only intended as an interim measure until a suitable off-site national repository is designed. HOSS would involve the following:

- The irradiated fuel older than five years – which represents the vast majority of the fuel in the pools – should be placed in robust dry storage casks. Stored in hardened casks and dispersed and shielded appropriately, the irradiated fuel is less vulnerable to an irradiated fuel fire triggered by accident, sabotage or terrorist attack.

[2] A nuclear reactor core contains a number of fuel assemblies, bundles of thin tubes containing pellets of enriched uranium. These tubes are usually referred to as fuel rods. Over time, the buildup of neutron-absorbing poisons resulting from the chain reaction reduces the ability of the fuel to sustain an efficient chain reaction, and the rods must be replaced.

[3] Concept conceived by Dr. Arjun Makhijani, President of the Institute for Energy and Environmental Research.

- The remaining irradiated fuel assemblies in the pool should be reconfigured so that the density is reduced and there is more space in between each assembly. The current spacing between fuel assemblies in the pool is dangerously close which increases the probability of an irradiated fuel fire. It also increases the likelihood that the fire would engulf more fuel and release greater amounts of radioactivity.

- Containment buildings, above-ground bunkers or berms should be used to shield the dry storage casks from line-of-sight so that the casks are not vulnerable to acts of terrorism involving hand-held weaponry (i.e. anti-tank missiles) or airplanes. If the current proposal is implemented, Entergy would ultimately have 53 casks situated together -- fully exposed -- on a concrete pad, and possibly many more casks if the NRC grants Entergy's request for a 20-year license renewal. With the casks stored in such a vulnerable manner, a terrorist attack involving a plane crash could destroy several casks and release radioactive material.[4]

- A robust, containment structure should be built over the existing irradiated fuel pools. The buildings that currently house each irradiated fuel pool at Indian Point do not serve as containment; nor are they fortified structures capable of repelling a terrorist attack.

While the U.S. drags it feet with respect to the need to better protect irradiated fuel, other nations have taken important steps to fortify irradiated fuel storage. One particular facility, the Gorleben nuclear fuel center in the German state of Lower Saxony, has a building which is licensed to hold 420 casks containing about 4200 tons of uranium in irradiated fuel. The walls and roof of the Gorleben building are about 50 and 15 cm thick reinforced concrete, respectively.[5]

2) Install Passive Defense Systems: Different types of passive defense systems can be deployed at nuclear power plants which would go a long way towards thwarting air-based attacks. Examples include:

- **Beamhenge:** Beamhenge[6] should be installed at Indian Point in areas where postulated aerial attack impacts could result in damage to the reactor, spent fuel storage systems or other vulnerable targets like the steam lines running between the reactor and turbine buildings. Beamhenge is a line of steel beams set vertically in deep concrete foundations connected by bracing beams, a web of high-strength cables, wires, and netting linking the vertical beams to form a protective screen – the nuclear-grade equivalent of the fences erected around golf driving ranges.

---

[4] Gordon Thompson, *Robust Storage of Spent Nuclear Fuel: A Neglected Issue of Homeland Security* by Institute for Resource and Security Studies. (January 2003)

[5] Alvarez et al, "Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States," published in the journal *Science and Global Security*. (Spring 2003)

[6] Source: The May/June issue of the Bulletin of the Atomic Scientists features an article on nuclear power plant security written by Dave Lochbaum, Ed Lyman and Daniel Hirsch. The article is titled "THE NRC's DIRTY LITTLE SECRET: The Nuclear Regulatory Commission is still unwilling to respond to serious security problems." See sidebar article by Joel Hirsch, titled "Beamhenge." The article can be viewed at: **http://www.thebulletin.org/issues/2003/mj03/mj03hirsch.html#Anchor-Special-49575**

Beamhenge would not need to completely encircle the nuclear plant - it would merely need to shield the vulnerable side or sides of the facility's key structures. Depending on the nuclear plant's geography and vulnerabilities, Beamhenge could be a single row of closely spaced beams or multiple rows of more widely spaced beams. The height of the beams and the length of the Beamhenge would depend on the configuration of facilities being protected from likely incoming trajectories.

The main purpose of Beamhenge would be to slow down an attack, fragment the attacking aircraft into smaller pieces, disperse the mass of jet fuel, and protect the more vulnerable containment, spent fuel pool, and other structures located within the perimeter from being breached by the mass of the projectiles. The beams would tend to scatter the jet fuel and slow down other projectiles like the fuselage.

The structure would also provide some degree of protection against surface-to-surface and air-to-surface missiles, as well as other ballistic and self-propelled ordnance. The metal mesh netting strung between the vertical beams would not stop a projectile, but would serve to trigger detonation of its warhead before it reached the facility's walls.

- **Earth Berms:** Earth berms protect against attacks by rocket-propelled grenades, anti-tank missiles, aircraft attacks and many other possible scenarios. Berms can be used to protect various soft targets onsite including the dry casks that house spent fuel.

- **Dunlop Barriers:** Dunlop barriers should be installed in the Hudson River around Indian Point's exclusion zone to help protect such vulnerable targets as the cooling water intake structures. Dunlop barriers are inflated cylinders of a rubber-coated textile and are linked together or to a mooring buoy to form a security barrier around an exclusion zone. They can be used to thwart small-boat terrorist attacks. These barriers have already been put in place at several Navy bases.

3) Establish Combat Air Patrols and No Fly Zones: Until the passive defense systems are in place, a no fly zone should be imposed around the Indian Point nuclear power plant. Commercial and private aircraft should be prohibited from flying within 10 nautical miles or below 18,000 feet above 100 sensitive sites around the nation, including Indian Point. This would apply to commercial planes, private planes and helicopters.

No fly zones should be coupled with requiring the Department of Defense and the relevant departments to a) establish regular combat air patrols (CAP) over the Indian Point plant and b) conduct air intercept drills which include scenarios under which the potential target is Indian Point. These two measures were called for by Senator Hillary Clinton late last year.

News reports indicate that the FBI and the Department of Homeland Security have warned government and industry officials to be on guard against Al Qaeda operatives hijacking cargo jets in Canada, Mexico or the Caribbean and then flying them into this country to attack nuclear plants and other critical infrastructure.

By the government's admission, there remains no air defense for Indian Point other than "improved security at our nation's airports" (which still has a long way to go). There are no specific measures in place that would protect Indian Point from an aerial assault either by a jumbo jetliner or a small plane coming from one of the region's poorly secured airports. A no fly zone exists over Disney World and Disneyland but not over Indian Point. While hitting the containment domes with a commercial airliner could penetrate the domes and lead to a meltdown, a more vulnerable target would be the spent fuel pools.

4) Bolster Water-based Security: Coast Guard and naval militia presence on the water in front of the plant must be full-time. They must be armed with the appropriate technology and weaponry to thwart a water-based attack.

5) Augment Security Forces: The number of National Guard troops at Indian Point should be increased with a special focus on protecting the plant's more vulnerable targets such as the spent fuel storage systems.

6) Maintain Highest Alert Status for Indian Point: At all times, the Indian Point nuclear power plant should remain at the highest alert status.

7) Revamp Federal Policies and Regulations: Congress must revamp the NRC and FEMA's policies and regulations governing nuclear plant security and emergency preparedness. These agencies have stacked the deck against public interest groups and other parties who have tried to raise legitimate concerns regarding plant safety and security. The NRC's policies provide the most egregious example of government attempts to impede public participation. In several recent proceedings the NRC has argued that since terrorism is too speculative under the NEPA process, the issue of terrorism cannot be raised in site-specific proceedings such as license renewal.

Before making several recommendations, I'd like quickly address the issue of relicensing in more detail. It should go without saying that the license renewal issue raises several significant safety, security and environmental issues that affect not only the residents of the Hudson Valley, but impact the health and safety of those living and working in the greater New York City metropolitan area. The people of this region are all too familiar with the risks of global terrorism, and the potential twenty year extension of Indian Point's license must be considered in light of domestic security and emergency preparedness.

Furthermore, given the plant's aging condition and its close proximity to millions of residents, the extension request must be subjected to a heightened level of scrutiny. Given the significant increase in the local and regional population, as well as the heightened threat environment, the relicensing process must ask the basic question of whether this plant should continue to operate. Today, there are still too many questions and concerns about the security of the facility, its vulnerability to terrorist attack, its emergency response capability, as well as its underlying operation condition.

Specifically, we seek congressional support in challenging the manner in which the NRC handles the issue of terrorism and its relevance to NEPA.

We urge your leadership in Congress to ensure the passage of legislation that:

a) Requires that a NEPA analysis specify that licensing requests need to be evaluated for environmental impacts associated with acts of terrorism on a nuclear power facility.

b) Requires the NRC process license renewal requests as if they were new reactor proposals. This would ensure that antiquated studies, such as that regarding the seismic hazard threat to a plant, are not used as the basis for justifying an additional 20 years of operation. For the sake of argument, if Entergy chose to immediately close Indian Point's existing reactors and seek to replace them with new reactors, the new reactors would clearly have to meet the NRC's new and more stringent seismic criteria (10 CFR Part 100.23 deals with geologic and seismic siting criteria). The same stringent criteria pertaining to new reactors should also apply to existing reactors, like those at Indian Point, that are seeking a 20-year license renewal. It is unclear whether such stringent criteria are being applied to Indian Point.

c) Requires the NRC, during its review of an applicant's request for license renewal, to examine the adequacy of the radiological emergency plan especially in cases as unique as Indian Point's and to publicize the criteria it employs to determine whether an emergency plan is adequate to protect public health and safety..

d) Requires the NRC's current DBT to be upgraded in order to ensure that plant security will be able to thwart an assault by a substantial number of terrorists. For decades, many experts have advocated for a significantly upgraded DBT which would require protection against 20 outside attackers working in conjunction with one active insider. Today that recommendation seems logical since there were 19 terrorists involved in the highly coordinated, technologically advanced September 11 attacks. Indian Point should be required to defend and capable of defending against a highly coordinated, technologically advanced attack involving 20 suicidal attackers entering the site from multiple directions and working with one inside conspirator.

e) Given the increased terrorist threat level, Indian Point's poor record on security, and the NRC's weak oversight, now is the time for greater scrutiny, not less. The NRC should reconsider its new policy on shielding security evaluations from the public. The NRC should implement an alternative policy that will allow nuclear watchdogs and public interest groups to participate in the development of security regulations and provide oversight in a manner that enhances security. Among the actions the NRC can take:

> i) Re-institute the pre-09/11 practice of publicly reporting high-level results from NRC security inspections at nuclear plant sites. Such results include the proper protection of specific information about exploitable weaknesses.
>
> ii) Re-institute the practice of routine public meetings on security policy issues.

f) The Department of Homeland Security (DHS) should be granted the authority to issue legally binding orders to the NRC, among other agencies, and the ability to enforce them through inspections and punitive actions. Currently, DHS lacks this authority and the agencies'

"infrastructure protection" function has been relegated to an advisory role that the NRC is free to ignore. Failing to provide DHS with this authority was not an inadvertent omission.

IV. CONCLUSION

Little has changed since 9/11 regarding the level of security at Indian Point. In general, nuclear plant security only has been improved at the margins. Much of the upgrades to plant security are simply window dressing to give the illusion that security concerns are being taken seriously. Security officers inform us that in many cases, the problems have actually worsened at Indian Point.

Federal agencies remain in a state of denial and it is becoming increasingly apparent that the root of this denial is their bias toward protecting industry profits at the price of public safety.

At the very least, there are a number of obvious measures that the NRC should be able to support that would not present an economic burden to plant operators. It is not clear why the NRC has not called for such improvements, but one possibility is that the industry doesn't want more visible security measures to raise questions among the public about the intrinsic safety of nuclear power, especially not at a time when the industry is hoping to build a whole new generation of plants.

The federal government's current approach to nuclear plant security and emergency preparedness is leading us down a path that will result in far worse consequences than the tragedy of September 11th. We have received the warning signs regarding the possibility of and our vulnerability to a terrorist attack on a U.S. nuclear power plant, much as the government had received warnings about the 9/11 attacks. Let's not give a future 9/11-type commission the opportunity to say we knew an attack on a nuclear plant was possible and did too little to stop it or minimize the impacts.

Thank you for the opportunity to participate in this hearing.

ATTACHMENT A

EXECUTIVE SUMMARY
(from the report "Chernobyl-on-the-Hudson?: The Health and Economic Impacts of a Terrorist Attack at the Indian Point Nuclear Plant.")

Since 9/11, the specter of a terrorist attack at the Indian Point nuclear power plant, thirty-five miles upwind from midtown Manhattan, has caused great concern for residents of the New York metropolitan area. Although the Nuclear Regulatory Commission (NRC) ordered modest security upgrades at Indian Point and other nuclear power plants in response to the 9/11 attacks, the plants remain vulnerable, both to air attacks and to ground assaults by large terrorist teams with paramilitary training and advanced weaponry. Many question whether the NRC's security and emergency planning requirements at Indian Point are adequate, given its attractiveness as a terrorist target and the grave consequences for the region of a successful attack.

This report presents the results of an independent analysis of the health and economic impacts of a terrorist attack at Indian Point that results in a core meltdown and a large radiological release to the environment. We find that, depending on the weather conditions, an attack could result in as many as 44,000 near-term deaths from acute radiation syndrome or as many as 518,000 long-term deaths from cancer among individuals within fifty miles of the plant. These findings confirm that Indian Point poses a severe threat to the entire metropolitan area. The scope of emergency planning measures should be promptly expanded to provide some protection from the fallout from an attack at Indian Point to those New York area residents who currently have none. Security at Indian Point should also be upgraded to a level commensurate with the threat it poses.

A 1982 study by Sandia National Laboratories found that a core meltdown and radiological release at one of the two operating Indian Point reactors could cause 50,000 near-term deaths from acute radiation syndrome and 14,000 long-term deaths from cancer. When these results were originally disclosed to the press, an NRC official tried to reassure the public by saying that the kind of accident the study considered would be less likely than "a jumbo jet crashing into a football stadium during the Superbowl."

In the post-9/11 era, the possibility of a jumbo jet crashing into the Superbowl --- or even a nuclear power plant --- no longer seems as remote as it did in 1982. Nonetheless, NRC continues to argue that the 1982 Sandia report is unrealistic because it focused on "worst-case" accidents involving the simultaneous failure of multiple safety systems, which are highly unlikely to occur by chance. But when the potential for terrorist attacks is considered, this argument no longer applies. "Worst-case" scenarios are precisely the ones that terrorists have in mind when planning attacks.

Both NRC and Entergy, the owner of Indian Point, assert that even for the most severe terrorist attack, current emergency plans will be adequate to protect residents who live in the evacuation zone within 10 miles of the plant. They also say that there will be no significant radiological impact on New York City or any other location outside of the 10-mile zone. Accordingly, NRC has opposed proposals made after 9/11 to extend the emergency planning zone around Indian

Point. However, NRC and Entergy have not provided the public with any documentation of the assumptions and calculations underlying these claims.

In view of the lack of public information available on these controversial issues, we carried c an independent technical analysis to help inform the debate. Our calculations were performe with the same state-of-the-art computer code that NRC uses to assess accident consequences We used the NRC's guidance on the radiological release from a core meltdown, current estimates of radiation risk, population data from the 2000 census, and the most recent evacuation time estimate for the 10-mile Indian Point emergency planning zone. Following the format of the 1982 Sandia report, we calculated the numbers of near-term deaths from acute radiation syndrome, the numbers of long-term deaths from cancer, and the maximum distance at which near-term deaths can occur. We evaluated the impact of both evacuation and sheltering on these outcomes. We also estimated the economic damages due to the long-term relocation of individuals from contaminated areas, and the cost of cleanup or condemnation of those areas.

The health and environmental impacts of a large radiological release at Indian Point depend strongly on the weather conditions. We have carried out calculations for over 140,000 combinations of weather conditions for the New York area and wind directions for the Indian Point site. For this data set, we have determined the average consequences, the peak consequences, and the consequences for "95th percentile" weather conditions (in other words, only 5% of the weather sequences analyzed resulted in greater consequences).

We believe that the 95th percentile results, rather than the average values, represent a reasonable assessment of the likely outcome of a successful terrorist attack, since such attacks would most likely not occur at random, but would be timed to coincide with weather conditions that favor greater casualties. Attacks capable of causing the peak consequences that we calculate would be difficult to achieve because of inaccuracies in weather forecasts, restricted windows of opportunity and other factors, but remain within the realm of possibility.

For a successful attack at one of the two operating Indian Point reactors, we find that

- The number of near-term deaths within 50 miles, due to lethal radiation exposures received within 7 days after the attack, is approximately 3,500 for 95th percentile weather conditions, and approximately 44,000 for the worst case evaluated. Although we assumed that the 10-mile emergency planning zone was entirely evacuated in these cases, this effort was inadequate because (according to Entergy's own estimate) it would take nearly 9.5 hours to fully evacuate the 10-mile zone, whereas in our model the first radiological release occurs about two hours after the attack.

- Near-term deaths can occur among individuals living as far as 18 miles from Indian Point for the 95th percentile case, and as far as 60 miles away in the worst case evaluated. Timely sheltering could be effective in reducing the number of near-term deaths among people residing outside of the 10-mile emergency planning zone, but currently no formal emergency plan is required for these individuals.

- The number of long-term cancer deaths within 50 miles, due to non-acutely lethal radiation exposures within 7 days after the attack, is almost 100,000 for 95th percentile weather conditions and more than 500,000 for the worst weather case evaluated. The peak value corresponds to an attack timed to coincide with weather conditions that maximize radioactive fallout over New York City.

- Based on the 95th percentile case, Food and Drug Administration guidance would recommend that many New York City residents under 40, and children in particular, take potassium iodide (KI) to block absorption for radioactive iodine in the thyroid. However, there is no requirement that KI be stockpiled for use in New York City.

- The economic damages within 100 miles would exceed $1.1 trillion for the 95th percentile case, and could be as great as $2.1 trillion for the worst case evaluated, based on Environmental Protection Agency guidance for population relocation and cleanup.

We hope that this information will be useful to Federal, State and local homeland security officials as they continue to develop plans to protect all those at risk from terrorist attacks in the post-9/11 world.

Mr. SHAYS. Mr. Lochbaum.

Mr. LOCHBAUM. Thank you Mr. Chairman. I appreciate this opportunity to present our views on nuclear power plant security.

Today's open hearing demonstrates that nuclear plant security issues can be responsibly discussed in public, a fact lost upon the Nuclear Regulatory Commission. The NRC essentially closed its doors to the public on this important topic since September 11. That's unacceptable, and we urge the Congress to compel the NRC to follow its lead by including the public in policy discussions.

Mr. SHAYS. That's a very interesting point. It has never occurred to me that it's being used. The irony is it is being used as an excuse not to have the dialog when we need the dialog even more.

Mr. LOCHBAUM. But it is also forcing groups like ours to go to other avenues since they have closed our doors, and the media and other outlets are the way we find our voice since they have closed our voice. They would probably prefer that they had those comments in house than seeing them in headlines.

Mr. SHAYS. Good point.

Mr. LOCHBAUM. A successful attack on a nuclear power plant would be one of the worst disasters in American history. That this threat is real is revealed by two simple facts. First, the nuclear industry urged this Congress to renew Price-Anderson Federal liability protection for nuclear power plants. If an attack could not cause catastrophic harm, owners could get private insurance coverage.

Second, the nuclear industry claims to have spent more than $1 billion upgrading security since September 11. No one has enough money to spend on pseudo threats.

After September 11, the industry issued orders requiring plants to take steps to make facilities less vulnerable to attack.

The NRC also revamped its oversight process. The steps we liked most among them are frequency of NRC-evaluated force-on-force security test was increased to once every 3 years from once every 8 years, the number of design basis threat adversaries was increased, and many of the unrealistic limitations on their weapons and tactics were lessened or removed.

Minimum standards have been established for training and qualifications of security force personnel, and working hour limits for security force personnel were mandated by the NRC.

Despite these steps taken, nuclear power plants remain vulnerable to attack by land, sea and by air. The American public cannot honestly be assured that all reasonable measures to protect them have been taken until the following 10 steps are taken:

The two-person rule and/or expanded in-plant use of security monitoring cameras needs to be done to better control vital access to areas.

The evaluation process for proposed procedure revisions and hardware modifications must formally verify whether protection against sabotage is affected by the planned changes.

The NRC must not allow the same company to provide both the attackers and the defenders in force-on-force security tests.

The NRC must increase its design basis threat level to a realistic level comparable to that established by the DOE after September 11.

The NRC must either require background checks for nuclear plant workers with access to sensitive plant information or to prevent these workers from accessing that information.

The NRC must require water barriers around intake structures at nuclear power plants.

The NRC must require protection against aircraft hazards similar to the process it used to protect the plants against fire hazards.

The Federal Government's ability to withstand or respond an attack designed above the design basis threat level must be periodically demonstrated.

The NRC must require adequate protection for spent fuel by requiring owners to transfer fuel discharged from the reactor more than 5 years ago into dry casks which are emplaced within earth berms and other protective devices.

And last—or, actually, first—the NRC must reengage the public in security policy discussions.

I would like to highlight two of those recommendations. The others are detailed further in my written testimony.

Right now, spent fuel at nuclear power plants is not as safe or as secure as it should be. Many plants have five to eight times as much spent fuel as fuel in the reactor. There are fewer barriers that attackers must penetrate in order to successfully damage spent fuel. And, correspondingly, there are fewer barriers protecting the public from the radioactivity released from damaged fuel.

At most plants, the spent fuel pools are filled to overflowing. Spent fuel is then loaded into dry casks and placed out on open air lots out back. In fact, the current scheme of spent fuel storage could hardly be made less safe or less secure. By maintaining the spent fuel pools at or near full capacity, the risk is kept as high as it possibly can get. Transferring spent fuel into dry casks merely adds the additional risk of spent fuel out in the backyard.

The responsible thing to do would be to minimize the inventory in spent pool fuels by transferring fuel discharged from the reactor more than 5 years ago into dry casks, which are then placed in earthen walls or other protective devices. The risk reduction by emptying the spent pool would more than offset the increased risk from dry cask storage resulting in overall tangible reduction in the risk profile at each plant site.

The second recommendation I will highlight involves access to sensitive information. As this subcommittee has discussed, the NRC's imposed restrictions as recently as August 4th on the public's access to information after September 11. But there is a huge loophole. The access authorization upgrades mandated by the NRC after September 11 only apply to nuclear plant workers who get unrestricted access. There are literally thousands of nuclear plant workers with ready access to sensitive plant information that do not get unescorted access and therefore are not subject to background checks. Our enemies can get those jobs and obtain blueprint calculations, risk assessment hazards and analysis and upcoming equipment outage schedules useful in planning an attack.

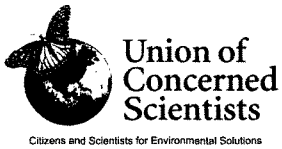
The NRC has to plug this loophole. It makes little sense to restrict public access to information while allowing the equivalent of uncontrolled drive-through service at the plants themselves.

Before I close, I would like to take a moment to defend the NRC from the chairman's concerns about the 6-year security upgrade schedule. That's actually the NRC's express lane. You should see their pace at resolving safety issues. By comparison, 6 years is the blink of an eye.

Mr. Chairman, I sincerely thank you for holding this open hearing and for listening to the public perspectives on this important issue.

Mr. SHAYS. Thank you.

[The prepared statement of Mr. Lochbaum follows:]



Statement Submitted by David Lochbaum to the Subcommittee on National Security, Emerging Threats, and International Relations, U.S. House of Representatives

Mr. Chairman and Members of the Subcommittee, I appreciate this opportunity to provide you with our views on the important public policy issues associated with nuclear power plant security. I have been the nuclear safety engineer for the Union of Concerned Scientists since October 1996. I worked for over 17 years in the nuclear power industry prior to joining UCS. As a Shift Technical Advisor, I stood – albeit very nervously – inside the control room at the Browns Ferry nuclear plant as the deadline for a phoned-in bomb threat approached and then passed without incident. I authored the investigative reports into a series of mysterious shutdowns of the Browns Ferry reactors caused by a group of workers tampering with vital safety equipment to sabotage the plant.

Today's open Congressional hearing, as with many others that preceded it, demonstrates that nuclear plant security issues can be responsibly discussed in public – a fact ignored by the U.S. Nuclear Regulatory Commission (NRC). The NRC has essentially closed its doors to the public on this important topic since 09/11. That's unacceptable and we urge the Congress to compel the NRC follow its lead by including the public in policy discussions.

Nuclear Plant Security Hazard is Real

Nuclear industry representatives and NRC officials often state that any attack on a nuclear power plant would not and could not harm people living and working outside its fences. Those statements mislead the public, undermine confidence in nuclear plant security preparedness, and are disrespectful to the thousands of Americans working long hours to prevent a successful attack. The truth is that a successful attack on a nuclear plant would be one of the worst disasters in American history. The utter fallacy of their statements is perhaps best revealed by two facts. First, the nuclear industry and the NRC urged Congress to renew Price-Anderson federal liability protection for nuclear power plants. If an attack could not cause harm outside nuclear plant fences, owners could get private insurance coverage and would not need Price-Anderson. Second, the nuclear industry claims to have spent more than $1 billion upgrading nuclear plant security since 09/11. No one spends that kind of money on pseudo-hazards.

Security Steps Taken

UCS acknowledges that the NRC embarked on a campaign before 09/11 to upgrade nuclear plant security requirements and their implementation. In two policy papers supplied to the Commissioners in June 2001, the NRC staff enumerated many proposed revisions to the nuclear plant security regulation (10 CFR 73) and how the agency would better enforce it. The NRC staff prepared these policy papers following a lengthy series of monthly public meetings. Thus, the NRC had a solid foundation to build upon when the tragic events of 09/11 forced reconsideration in light of this new threat to our homeland.

With the pre-09/11 preparation and post-09/11 perspective, the NRC issued a series of orders to plant owners requiring them to take steps to make their facilities less vulnerable to attack. The NRC also revamped its own processes for determining the adequacy of security measures. The steps we like the most:

- The frequency of NRC-evaluated force-on-force security testing was increased to once every three years from once every eight years.

  NOTE: UCS shares the concern expressed by the Project on Government Oversight (POGO) about the obvious conflict-of-interest in having Wackenhut employees serve as both the attackers and defenders during force-on-force tests as currently planned by the Nuclear Energy Institute. The NRC must not permit this farce.

- Access authorization procedures for plant workers were upgraded to prevent unescorted access *before* the FBI fingerprint check results come back, to require background checks to be updated every five years, and to restrict access by temporary workers with only cursory background checks.

- The number of adversaries in the design basis threat (DBT) was increased and many of the unrealistic limitations on their weapons and tactics were removed or lessened.

  NOTE: UCS shares the concern expressed by virtually every public interest group that the modest increase in the number of adversaries may be insufficient because it remains far below the DBT level developed by the Department of Energy after 09/11 for its nuclear facilities with comparable hazards.

- Minimum standards for training and qualifications of security force personnel were established to ensure these personnel are capable and equipped.

- Working hour limits for security force personnel were mandated to protect these workers from impairment by fatigue.

The steps taken by the NRC since 09/11 made it less likely that an attack against a nuclear power plant will be successful. But the nuclear plants have not, by any stretch of the imagination, been made invulnerable. We must not gamble that our enemies are too inept to exploit the vulnerabilities. September 11th reminded us the stakes from losing this gamble are tragically high.

Security Steps Remaining
Nuclear plants are vulnerable to attack from the land, the water, and the air. Additional steps must be taken to reduce all three vulnerabilities.

Land-based attacks can come from within the security fences, from outside the fences, and from a combination of inside and outside attacks. The NRC reduced the threat of insider sabotage by revising access authorization procedures after 09/11, but two additional low-cost measures must be taken. First, access to vital areas[1] must be controlled better. The United States military applies the "two-person" rule for entry into areas containing key components of the atomic arsenal to make theft and tampering less likely. Likewise, the "two-person" rule for access to vital areas and/or expanded use of in-plant security monitoring cameras will lessen the likelihood of sabotage by insiders at nuclear plants. Many vital areas (e.g., the electrical switchgear rooms and the instrument rooms) are low-traffic areas that can be further protected by the "two-person" rule. Other vital areas (e.g., the control rooms) are high-traffic areas that are better protected by monitoring using in-plant cameras. These low cost measures[2] would further reduce the likelihood of insider sabotage by better controlling access to areas containing vital equipment.

The second low-cost measure against insider sabotage involves expanding the evaluation process for proposed procedure revisions and hardware modifications to formally include sabotage threat. Currently, proposed changes are formally evaluated per 10 CFR 50.59 to verify that safety levels will not be

---

[1] The NRC terms the land under and around a nuclear plant the owner-controlled area. The subset of that area demarked by the inner security fences is the protected area. The rooms within the plant containing equipment necessary to protect the nuclear fuel are vital areas. Most workers perform their assigned duties outside of the vital areas.

[2] UCS has not quantified the cost implications of these measures, but qualitatively compared them to practices currently in place at nuclear power plants. There are confined space entry requirements that a worker from entering a tank or other area alone or unmonitored where conditions may pose a health hazard. There are security cameras used to monitor exterior perimeters. The extension of these existing measures to better protect vital areas is relatively inexpensive.

compromised. If the formal evaluation cannot determine that safety levels will be maintained, then NRC approval of the proposed changes is required. This evaluation process must be expanded to ensure that proposed changes that do not lessen safety levels also do not make it easier for insiders to sabotage the plant. For example, continued plant operation with one of two redundant emergency pumps intentionally disabled a few days for maintenance might be justified from a safety perspective based on the small chance of an accident occurring during that brief period along with the high reliability of the remaining pump. But continued plant operation might not be justified in this case from a security perspective without taking compensatory measures to protect the remaining pump from sabotage during the brief period. This low cost measure[3] would further reduce the likelihood of insider sabotage.

The best protection against land-based attacks originating outside the fences involves periodic, meaningful force-on-force security tests at a realistic DBT level. The NRC has adequately addressed the periodicity by increasing the testing frequency to once every three years. The NRC must address the meaningfulness by not allowing Wackenhut – or any other private company – from supplying both the attackers and defenders in a security test. There is a clear conflict-of-interest that must not be permitted. The NRC must address the realistic DBT level by increasing the current modest level to at least the level established by the DOE following 09/11 for its nuclear facilities.

Limiting access to plant information protects against external land-based attacks by impairing the ability of outsiders to identify targets and devise tactics. The NRC imposed additional restrictions, as recently as August 4, 2004, on public access to information after 09/11. But UCS met privately with the NRC staff in May 2004 to point out a significant loophole. The beefed-up access authorization steps mandated by the NRC following 09/11 only apply to nuclear plant workers who are granted unescorted access privileges. There are literally thousands of nuclear plant workers with ready access to sensitive plant information that do not get unescorted access and therefore are not subject to background checks. It remains easy for our enemies to get these jobs and obtain blueprints, scale drawings, calculations, risk assessments, upcoming equipment outage schedules, and other information extremely useful in planning and executing an attack. The NRC must plug this loophole. It makes little sense to restrict public access to information while allowing the equivalent of uncontrolled, unmonitored, unfettered drive-thru service at the plants themselves.

Water-borne attacks seek to disconnect the nuclear plant from its adjacent lake, river, or ocean and prevent cooling of essential equipment and irradiated fuel. Very little has been done to protect nuclear plants from water-borne attacks. The United States Navy reacted to 09/11 by installing floating barriers around ships at anchor in U.S. ports. For example, the Navy placed floating barriers, provided by Dunlop Industries of Scotland at a cost of $10,000-15,000 per section, around its submarines in Groton, Connecticut as protection against its DBT. The NRC must require similar protective measures for the intake structures at nuclear power plants.

Air attack threats must be resolved via the same process the NRC applied to fire hazards following the near-disastrous Browns Ferry nuclear plant fire in 1975. The NRC required owners to analyze their plants area by area to verify that a fire disabling all of the equipment inside one area left sufficient undamaged equipment in the other fire to safely shut down the reactor. The NRC must also require owners to analyze their plants aircraft impact area by impact area to verify that an aircraft disabling all of the equipment inside one area leaves sufficient undamaged equipment to safely shut down the reactor and prevent damage to spent fuel. During this analysis, results may reveal an unacceptable vulnerability that must be resolved by either making the impact area more robust or ensuring survival of necessary equipment in other areas – replicating the resolution process used during the fire hazards analyses. UCS and the

[3] This measure would be relatively inexpensive because it is a small expansion to the existing safety evaluation process. The current process requires a formal evaluation of the potential impact of proposed changes upon fire protection, chemical interactions, seismic loads, etc., would require minor effort to also cover the potential impact on insider sabotage prevention.

Mothers For Peace of San Luis Obispo jointly petitioned the NRC to make this happen, but our petition seems to have disappeared into some regulatory black hole.

It must not be forgotten that all of the steps taken and all of the remaining steps – even if taken – only protect against an attack up to the DBT level. Per 10 CFR 50.13, the so-called "enemies of the state" regulation, the U.S. government is responsible for dealing with attacks above the DBT level. The federal government resources that would be deployed to prevent or respond to an attack against a nuclear plant on our coastlines are different than those deployed in event of an attack against a nuclear plant in Kansas. In this regard, protection above the DBT level is analogous to the emergency planning requirements contained in 10 CFR 50.47. A large-scale accident at a nuclear power plant challenges the resources and surpasses the authority of its owner to cope with areas outside of the facility's fences. The plant owner is required to have procedures to interface with local, state, and federal entities so they can make informed decisions necessary to protect downwind populations. During mandated biennial exercises, the NRC evaluates the plant owner and the Federal Emergency Management Agency (FEMA) evaluates the local, state, and federal entities on the effectiveness of their emergency planning measures.

A comparable process must be used to periodically demonstrate that the federal government could adequately prevent or respond to attacks above the DBT level. The frequency need not be as often as once every two years as in the emergency planning arena and the Department of Homeland Security would replace FEMA in evaluating offsite response. But periodic exercises would assure that necessary lines of communication were established and that roles and responsibilities were clearly understood so that the federal government's response to an imminent or actual attack on a nuclear plant was not an *ad hoc* effort.

Prior to 09/11, the NRC's security focus was on ensuring the irradiated fuel in the reactor was protected from damage by sabotage. That focus was incomplete. Many U.S. nuclear power plants have more than five times as much irradiated fuel in spent fuel pools and spent fuel dry casks as is in the reactor. There are substantially fewer barriers that saboteurs must penetrate in order to successfully damage spent fuel and, correspondingly, there are fewer barriers protecting the public from radioactivity emanating from damaged spent fuel. It is essential, therefore, to also assure that spent fuel is adequately protected.

Today, spent fuel at U.S. nuclear power plants is woefully protected. Spent fuel pools are filled to overflowing with irradiated fuel. Spent fuel dry casks are stored out in the open in direct light-of-sight to areas easily accessible by the public and people contemplating harm. In fact, the current scheme of spent fuel storage maximizes the risk from both accidental and intentional damage to spent fuel and could hardly be made less safe or less secure. By maintaining the spent fuel pools at or near full capacity, the risk is kept as high as possible.[4] Transferring irradiated fuel assemblies into dry casks stored on open-air concrete pads merely adds risk to the maximized spent fuel pool risk.

The responsible thing to do would be to minimize the inventory of irradiated fuel in the spent fuel pools by transferring fuel discharged from the reactor more than five years ago into dry casks emplaced within earthen berms or other protective devices. The risk reduction from emptying the spent fuel pool would more than offset the increased risk from dry cask storage, resulting in an overall tangible reduction in risk profile at the plant site. UCS joined a coalition of local and national organizations in petitioning the NRC last month to reduce the spent fuel storage risk at the most vulnerable nuclear plants – the boiling water reactors with Mark I containment designs. The NRC must take steps to adequately protect spent fuel.

These recommended steps would further reduce the vulnerability of nuclear power plants to attack. Even if fully implemented, they will not render nuclear plants invulnerable to attack. But at least these steps will allow the federal government to sincerely tell the American public following a successful attack, should one occur, that every reasonable step had been taken to protect them. Right now, Americans cannot be honestly given that assurance despite the NRC's steps since 09/11.

---

[4] The risk factors are described on page 15 of U.S. General Accounting Office report GAO-03-426, "Spent Nuclear Fuel: Options Exist to Further Enhance Security," July 2003.

Public's Right to Know
One of the first steps taken by the NRC after 09/11 was to bar the public from meaningful participation in policy discussions about nuclear plant security. The NRC has not yet retreated from this mis-step.

UCS supports the need for NRC to restrict public access to certain security information and that these restrictions are larger now. In fact, UCS identified materials containing security information in the NRC's electronic library both before and after 09/11 that we felt unsuitable for public consumption. We alerted the NRC to these materials and they have been pulled from the public arena. UCS actively supports the NRC's need to restrict public access to certain information.

Today's hearing demonstrates beyond reasonable doubt that open public discussions of nuclear plant security policy issues can be conducted responsibly. The NRC must learn this lesson and emulate this practice to begin repairing the damage inflicted by its mis-step. The American public is not the enemy. The NRC must stop treating the public as its enemy. The NRC cannot expect the American people to trust it when it displays a lack of trust in the American people.

Conclusion and Recommendations
Despite the steps taken by the nuclear industry and NRC since 09/11, nuclear power plants remain vulnerable to attack by land, by sea, and by air. There are additional steps that must be taken to reduce, but still not eliminate, these vulnerabilities. The American public cannot be honestly assured that all reasonable measures to protect them until after the following additional steps have been taken:

1. The "two-person" rule and/or expanded in-plant use of security monitoring cameras must better control access to vital areas.

2. The evaluation process for proposed procedure revisions and hardware modifications must formally assess whether protection against sabotage is affected by the planned changes.

3. The NRC must not allow the same company to supply both the attackers and the defenders in its force-on-force security tests.

4. The NRC must increase its DBT level to a realistic level comparable to the level established by DOE for its nuclear facilities after 09/11.

5. The NRC must either require background checks for nuclear plant workers with access to sensitive plant information or prevent workers without background checks from accessing sensitive plant information.

6. The NRC must require water barriers around intake structures at nuclear plants.

7. The NRC must require protection against aircraft hazards via a method like the one it employed to protect against fire hazards.

8. The federal government's ability to prevent or respond to an attack above the Design Basis Threat (DBT) level must be periodically demonstrated similar to how emergency planning preparedness for each nuclear plant site is periodically demonstrated.

9. The NRC must require adequate protection for spent fuel by requiring owners to transfer fuel discharged from the reactor more than five years ago into dry casks emplaced within earth berms or other protective devices.

10. The NRC must re-engage the public in security policy discussions.

Mr. Chairman and Members of the Subcommittee, I sincerely thank you for holding this open hearing and listening to public interest perspectives on this important topic.

Written testimony by David Lochbaum
Nuclear Safety Engineer
Union of Concerned Scientists
1717 H Street NW, Suite 600
Washington, DC 20006
(202) 223-6133
www.ucsusa.org

Mr. SHAYS. Mr. Fertel.

Mr. FERTEL. Thank you, Chairman Shays.

Given the importance of security at our nuclear plants today, I generally speak with the chief officers that operate those plants weekly, and I find I am getting to know a lot of the security managers personally. During the past 3 years, the industry has carried out unprecedented, unequalled efforts to review and improve our security; and I think during the discussion today the term business as usual, the lack of intensity and not exchanging lessons learned was used. I can only say that it's anything but business as usual. It's pretty intense, and we are exchanging lessons learned almost weekly. So I think there is a lot going on that I wish maybe we could share more with Dave and his colleagues.

I would like to start by emphasizing the importance of nuclear power to our Nation. Our Nation's 103 reactors safely and cleanly produce enough electricity to power one in every five homes and businesses in the United States. Many regions are heavily dependent on nuclear energy. For example, in the chairman's State of Connecticut, electricity from nuclear provides 50 percent of the power in that State; and these plants also provide an additional benefit of stabilizing the electricity grid.

I would like to emphasize three major points today regarding the security of our nuclear power plants:

First, nuclear power plants were the most secure industrial facilities in the United States before September 11th and against terrorist attacks, and they are even more secure today.

Second, power plants can serve as a model of industrial security in America. Our plants are far more secure than any other sector of our Nation's infrastructure and have been recognized as such by several independent organizations and security experts.

Third, while the industry is fully committed to protecting its employees, the public and its assets, our companies have maximized the level of protection they can reasonably provide to these facilities.

Although we coordinate extensively with government entities on security matters, continued emphasis on integrated response planning is necessary; and there are important legal and policy limitations to further increasing the security requirements that the operators of the plant have to satisfy.

As you know, nuclear power plants were built to be robust and secure. A nuclear reactor is secured by several feet of concrete walls and an internal barrier of steel reinforced concrete. They were built to contain the effects of a reactor accident and also to withstand natural accidents such as hurricanes, earthquakes, fires and floods.

Even before the September 11th attacks, every nuclear plant was protected by a strategy that included protective perimeters, physical barriers, sophisticated access authorization technology and a professional, well-armed security force. We conduct background checks on all of our employees and strictly control access to our plants.

After September 11th, the industry—in response to orders issued by the NRC—enhanced security at our plants significantly. Each

nuclear power plant is scheduled to meet the requirements of the most recent NRC security orders by the October 29th deadline.

Over the past 3 years, we have expanded our security force by 60 percent, from 5,000 to 8,000 security officers at the 64 sites. During that time, the industry has spent about $1 billion to increase the security force and to significantly enhance physical protection at the plant. About two-thirds of that or more is physical protection. So there are things happening at the plants.

My written testimony provides details regarding these improvements. However, some of them are considered safeguard information and thus not available to the public.

As part of the new security requirements, each plant will conduct multiple—and I repeat—multiple force-on-force exercises every year. The NRC formally evaluates each plant's force-on-force exercise at least once every 3 years, as you have heard before.

In these exercises, the NRC evaluates the execution of the security strategy, the performance of the plant security force and strategy, the performance of the plant security force and the performance of the independently trained adversary force used in the mock attacks.

I am looking forward to questions on why we hired Wackenhut, which I am sure we will get. We can talk about that. We think it is the right thing to do. We think it will enhance security at the plants.

Given the September 11th attacks, we also significantly increased our cooperation and coordination with State and local law enforcement. We have worked closely with the NRC, the Department of Homeland Security and other Federal, State and local authorities, with the goal of building a seamless security for our plants.

However, additional emphasis on integrated response planning is needed; and there are important legal implications to us doing certain things that we don't have the authority to do, that we need help from the governmental entities to do.

Mr. Matthiessen's testimony provides results from a new report by Riverkeeper on the consequences of possible terrific attack on the Indian Point nuclear power plant in New York. I just want to take a minute to discuss that report.

The industry always welcomes meaningful technical analysis of our nuclear facilities. However, this Riverkeeper report is more of the Hollywood equivalent of merging plots of "The Perfect Storm," "The Day After Tomorrow" and "Independence Day" and trying to sell it to the public as a realistic scenario. Simply, the likelihood of the accident sequence in this report leading to a release of radiation is so incredibly low that it is not credible.

With your permission, Mr. Chairman, I would like to include in the record an analysis of the Riverkeeper report recently prepared by leading technical experts. Thank you.

Mr. KUCINICH [presiding]. Thank you very much.

[The prepared statement of Mr. Fertel follows:]

Testimony for the Record

By
Marvin S. Fertel
Senior Vice President and Chief Nuclear Officer
Nuclear Energy Institute

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

September 14, 2004

1776 I STREET, NW SUITE 400 WASHINGTON, DC 20006-3708 PHONE 202.739.8000 FAX 202.785.4019 www.nei.org

TESTIMONY

MARVIN FERTEL
SENIOR VICE PRESIDENT AND CHIEF NUCLEAR OFFICER
NUCLEAR ENERGY INSTITUTE (NEI)

BEFORE THE
NATIONAL SECURITY, EMERGING THREATS
AND INTERNATIONAL RELATIONS SUBCOMMITTEE

COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 14, 2004

Chairman Christopher Shays, Ranking Member Dennis Kucinich, and distinguished members of the subcommittee, I am Marvin Fertel, senior vice president and chief nuclear officer at the Nuclear Energy Institute (NEI). I am honored to address the issues before this subcommittee today. As requested, I am here to discuss the nuclear energy industry's longstanding strengths—and its leadership—in American industrial security and how we have implemented yet more improvements in nuclear power plant security programs over the past three years.

NEI is responsible for developing policy for the U.S. nuclear industry. NEI's 270 corporate and other members represent a broad spectrum of interests, including every U.S. electric company that operates a nuclear power plant. NEI's membership also includes nuclear fuel cycle companies, suppliers, engineering and consulting firms, national research laboratories, manufacturers of radiopharmaceuticals, universities, labor unions, and law firms.

My testimony will address the following three issues:

- Nuclear power plants were the most secure industrial facilities in the United States before the Sept. 11, 2001, terrorist attacks. Nuclear plants are designed to withstand a broad range of events from tornadoes to earthquakes. Studies also have shown plants can withstand aircraft impacts on buildings and structures that directly house nuclear fuel, as well as ground-based attacks.

- The industry, responding to the Nuclear Regulatory Commission, has made nuclear power plants even more secure since September 2001. The industry has spent in excess of an additional $1 billion on security improvements and has increased its security forces by nearly 60 percent by hiring approximately 3,000 more security officers since Sept. 11. The NRC and industry have conducted numerous studies to ensure that plants are secure. The security at nuclear power plants is now at the limits of a private security force's capabilities.

- Further increases in the security requirements that are imposed upon the owners of nuclear power plants will have serious policy implications for overall homeland security. The nuclear industry supports legislation included in the energy bill conference report, that will enhance security at our plants and encourage Congress to enact those measures into law.

NUCLEAR POWER PLANTS ARE KEY TO ENERGY SECURITY AND CLEAN AIR

Prior to discussing the security provided at our plants, it is important to remind this subcommittee and Congress of the immense importance of nuclear energy to our country. Nuclear energy is a vital part of our nation's diverse energy portfolio, producing electricity—safely and cleanly—for one of every five U.S. homes and businesses. The United States remains the world leader in nuclear energy, with 103 reactors generating 764 billion kilowatt-hours of electricity in 2003—more than *all* of the electricity used in Great Britain and France combined. Our 103 reactors produce about one-fourth of the world's total nuclear-generated electricity.

Nuclear energy is the only large source of electricity that is both emission-free and readily expandable. The industry's exemplary safety record, outstanding reliability, low operating costs and future price stability make nuclear energy a vital source of power today and for the future. Nuclear energy is critical to U.S. energy security and diversity. Before the oil shocks of the early 1970s, nuclear power provided just 4 percent of our electricity supply, and oil provided about 20 percent. The situation is now reversed, as nuclear energy essentially has phased out oil use in the electricity sector. It would take 1.4 billion barrels of oil to generate as much electricity as nuclear energy produced in 2003, one-third of all the oil we import every year.

The steady growth of nuclear energy over the past three decades has produced enormous environmental and clean-air benefits. Nuclear energy now generates three-fourths of all emission-free electricity generation in the United States and is making significant reductions in harmful emissions into the atmosphere from the industrial sector. Nuclear power plants produce electricity that otherwise would be supplied by oil-, gas- or coal-fired generating capacity and thus avoid the emissions associated with fossil-fueled capacity.

Nuclear plants consequently have value in terms of compliance with various clean-air initiatives. In effect, emissions prevented through the use of nuclear energy are equivalent in value to those reduced as electricity is produced by other sources. Nuclear plants likewise help prevent the production of additional greenhouse gases, the most important of which is carbon dioxide (CO_2).

In 2002, President Bush proposed a voluntary program to reduce greenhouse gas intensity by 18 percent by 2012. Greenhouse gas "intensity" is a measure of tons of carbon per $1 million of gross domestic product. If current trends continue, U.S. greenhouse gas intensity will decrease 14 percent by that year—about 106 million metric tons, NEI estimates.

The U.S. nuclear industry is making the largest contribution by a single industry to greenhouse gas reduction. The nuclear industry estimates that it will add 10,000 megawatts through uprates and improved performance by 2012. This additional capacity will prevent the emission of about 22 million metric tons of carbon equivalent over the same period—more than one-fifth of the president's carbon reduction goal.

U.S. nuclear power plants prevented more than 750 million tons of carbon dioxide in 2003, which is equivalent to eliminating the CO_2 emissions from nine of 10 passenger cars in the United States—or about 134 million vehicles.

Nuclear power is essential in meeting clean air regulations. In 2002, U.S. nuclear power plants avoided the emission of about 3.4 million tons of sulfur dioxide (SO_2) and about 1.4 million tons of nitrogen oxide (NO_x). The requirements imposed by the 1990 Clean Air Act Amendments called for reductions of SO_2 emissions from the electric power sector between 1990 and 2002 by 5.5 million tons per year and reductions of NO_x emissions by 2.3 million tons per year. Thus, in a single year, using nuclear power plants to generate electricity has eliminated nearly as much in emissions as has been achieved over a 12-year period by all other sources combined.

According to a report issued last year by the Environmental Protection Agency and the Ozone Transport Commission, nuclear energy was one of the most significant compliance tools for reducing NOx emissions in northeastern and Mid-Atlantic states. The EPA assessment found that energy companies have been shifting electricity production from fossil-fueled power plants to emission-free nuclear power plants to help comply with federal air pollution laws.

NUCLEAR POWER PROVIDES ENVIRONMENTAL AND ECONOMIC BENEFITS TO THE NORTHEAST

The two nuclear reactors at the Millstone site produce over 50 percent of Connecticut's electricity and thus are vital to Connecticut's economic vitality. In addition, the six nuclear reactors in New York produce about 28 percent of that state's electricity, and Massachusetts receives over 13 percent of its electricity from nuclear power. Overall, the Northeast receives nearly a third of its electricity from nuclear power.

In addition, nuclear energy also is an environmental imperative for reducing greenhouse gases in specific regions of the country. New York is a good example of this phenomenon. New York's greenhouse gas emissions from fuel combustion decreased 1 percent from 1990 to 2002, despite a growth in population and the number of automobiles on the road. The increased production from the state's six nuclear power plants offset the need for electricity production at other power plants and therefore reduced greenhouse gas emissions during that period.

In 1990, the FitzPatrick, Ginna, Indian Point and Nine Mile Point nuclear power plants generated more than 24 billion kilowatt-hours of electricity in New York. By 2000, nuclear energy production increased by 60 percent, to more than 40 billion kilowatt-hours. This increase in nuclear production allowed for a decrease in the use of other fuels and offset an increase in emissions from the rising use of natural gas. The result is an overall 23 percent reduction in greenhouse gas emissions from the electricity sector.

As the New York example shows, nuclear energy is vital to our nation's clean-air programs. Expanding nuclear energy production through continued efficiency gains and building new nuclear plants would further enhance the role of nuclear energy in our environmental goals. Recent studies by the Earth Institute at Columbia University and the Massachusetts Institute of

Technology underscore the importance of nuclear energy and renewable energy sources in meeting energy and environmental goals that are inextricably linked.

Nuclear power plants are also vitally important to the local economies where they are located. According to a study prepared by NEI, the Millstone power plant, in New London County, Conn., employs nearly 1,500 people at salaries 50 percent higher than the local average. The plant paid $17 million in state and local taxes, including nearly one-fourth of all taxes paid to Waterford, Connecticut. In addition, the plant generated nearly 15 percent of all of New England's electricity needs and helped keep down energy prices in New England. Millstone did all of this without producing airborne emissions typical of other large-scale generation sources.

A similar study for the Indian Point Energy Center found that it employs nearly 1,700 people at significantly higher salaries than the averages for the surrounding counties. The economic activity generated by Indian Point creates an additional 1,200 jobs in the area. The center paid more than $25 million in taxes within Westchester County.

The Indian Point Energy Center meets approximately 11 percent of the total energy needs of the state of New York and plays a vital role in maintaining regional air quality. Estimates indicate that in the absence of Indian Point, the state's NO_x emissions would be 19 percent higher and SO_2 emissions would be 11 percent higher because fossil-fuel plants would offset Indian Point's production.

Some recommend closing the Indian Point Energy Center because of their concerns regarding security, but such a move would sacrifice a critical source of power for the state and needlessly reverse progress New York has made in reducing greenhouse gas emissions. EPA has determined that all five counties that surround Indian Point already do not comply with federal air rules. Taking Indian Point off the New York electricity grid would worsen air quality and unnecessarily drive up the cost of electricity to consumers and businesses.

The economic impact studies mentioned above are available on NEI's Web site at *www.nei.org*.

NUCLEAR PLANTS HAVE THE BEST INDUSTRIAL SECURITY IN THE NATION

Nuclear power plants are the most secure, commercially owned facilities in the country. We are justifiably proud of our security programs and the example they provide for America's industrial infrastructure. And we recommend that members of this subcommittee and any member of Congress visit one of our plants. I urge you to visit any plant in America that you choose, as they must all meet the same high standards set by the NRC.

Compared to other commercial facilities, nuclear power plants start with a clear advantage in the area of security. They were built to withstand certain natural events, such as earthquakes, hurricanes, tornadoes, fires and floods. They are massive structures with thick exterior walls and internal barriers of reinforced concrete. As such, the structures provide a large measure of protection against attacks. In addition, the "defense-in-depth" philosophy used in nuclear facility design means that plants have redundant and separated systems to ensure safety. That is, active

components, such as pumps, have backups as part of the basic design philosophy. This provides a capability to respond to a variety of events, including aircraft attack.

Our difficult-to-penetrate structures are only part of our security strategy. Nuclear power plants also have inner and outer perimeters with increased security at each level. We have physical barriers to protect against vehicle assaults, including truck bombs. Those perimeters are guarded by trained and armed professionals, who use hardened defensive fighting positions. Access to the vital areas of our plants is strictly controlled and constantly monitored.

Our employees are subjected to comprehensive background checks, a systematic fitness-for-duty program and a continual behavioral observation program to identify potential alcohol or drug abuse problems. Every plant also has extensive plans and arrangements to coordinate with state and local entitites. In addition, every plant must maintain a comprehensive emergency evacuation plan.

I have also made available a DVD produced by NEI on nuclear power plant security. Although many details of our security are considered "safeguards" and thus not open to public viewing, this DVD provides an excellent overview of the security employed at every nuclear plant. In addition, I have attached two NEI fact sheets on nuclear plant security and plant security improvements since Sept. 11. The security DVD and the fact sheets also are available on NEI's Web site at *www.nei.org*.

We believe that our plants' combination of hardened structures, perimeter protection, access controls and other security measures greatly exceeds the security provided at other commercially owned facilities, including many facilities that pose an equal and often greater threat to public safety from a terrorist attack than do nuclear power plants. The robust design and construction of nuclear plants and the multiple safe shutdown systems incorporated at each site make the likelihood, even from a terrorist attack, of a radiological release that would threaten public health extremely unlikely and well below other societal risks.

NRC, Industry Taking Decisive Steps to Verify Plants are Adequately Protected

The industry and the NRC have undertaken a series of decisive steps to reassess security programs and implement additional measures. These steps have included:

- a reassessment of industry security programs and the regulations governing them
- a plant-by-plant review of security programs, with every company responding
- significant investment in manpower and capital improvements to strengthen plant security
- major studies to reassess our plants' ability to withstand attack.

It is important to recognize the roles that the industry and our regulator, the NRC, play in providing security at our plants. The NRC mandates that each plant provide sufficient security to protect against the "design basis threat" (DBT), a regulatory definition of the abilities of a potential attacking force. Although this is accomplished by detailed orders and regulations, it is the responsibility of each company at each site to meet such requirements. The determination of

the potential risk to terrorist attacks—requiring the cooperation and coordination of our intelligence-gathering and federal law enforcement agencies—is a governmental function.

We recognize that there can be threats to our plants that are greater than what is defined by the DBT. Although our security would provide an initial deterrence, at some point such threats are the responsibility of the federal government, which has full intelligence, interdiction and military response capabilities. Since Sept. 11, 2001, the Department of Homeland Security (DHS) and the NRC have recognized the importance of coordinating federal, state and local authorities with the industry to best defend against such an attack. The DHS and NRC have conducted a pilot program to integrate the response planning around nuclear plant sites. The industry is participating in and fully supports this effort.

After 9/11, the NRC and the nuclear industry conducted studies to determine the vulnerability of nuclear power plants to various types of terrorist attacks. Although a nuclear plant would pose a well-defended, hardened target for any potential terrorist attack, these studies analyzed the risk to public health and safety that would result from a successful terrorist attack using a commercial airplane and assuming a successful ground assault on a nuclear plant. In both cases, the damage to the plant and the economy of the surrounding area would be significant, yet the actual risk to the public due to a release of radiation from the plant was determined to be extremely low.

THE NRC AND INDUSTRY HAVE SYSTEMATICALLY INCREASED AND IMPROVED SECURITY SINCE 9/11

As NEI noted last year before this committee, nuclear power plants, even before Sept. 11, 2001, were our nation's most secure private industrial facilities. Since then, we have greatly bolstered security at our plants—making them even more secure. Over the past three years, the nuclear energy industry has cooperated and worked with the NRC to review nuclear plant security completely, and many improvements have been implemented as a result.

Our first set of improvements took place on Sept. 11, 2001, when the NRC ordered all nuclear power plants to remain on high alert. We limited access to our plants. We expanded our protective perimeters. We constructed temporary barriers and discontinued non-essential activities. In addition, nuclear power plants immediately began hiring additional security personnel and upgrading overall security.

In February 2002, the NRC issued a number of interim security orders. These orders, in effect, increased the DBT, and the level of security at nuclear power plants was significantly increased in several areas. The industry, complying with the NRC orders, instituted additional measures, such as:

- extending and fortifying security perimeters
- increasing patrols within security zones
- installing new barriers to protect against vehicle bombs
- installing additional high-tech surveillance equipment
- strengthening security coordination with local, state and federal agencies to integrate approaches among the entities—a position the industry continues to support.

For the next several months after the issuance of the orders, the industry worked closely with the NRC to develop a guidance document to ensure consistent and thorough implementation of the new security requirements.

Following the completion of its top-to-bottom review and its study of the potential threats to nuclear power plants, the NRC issued the final DBT in April 2003. At that time, the NRC issued orders that enhanced training and qualification of security officers, improved access controls and established work-hour limits. These orders required licensees to develop and submit new security plans, training and qualification plans and safeguards contingency plans.

The new DBT increased security requirements on our plants in several ways. The potential vehicle bomb size was increased as was the number of terrorist attackers in a ground assault. The new DBT also increased the modes of attack to include water-borne assaults.

Each plant was ordered to make the necessary modifications to meet the new DBT by Oct. 29, 2004. To achieve this objective, the industry developed standardized templates for the new plans and obtained NRC concurrence on the templates for industry use. This innovative template approach not only assured the consistent implementation of the security orders but greatly facilitated NRC review of individual licensee security plans.

As a result of these new requirements, the number of security officers at our 64 plant sites has increased from approximately 5,000 to 8,000, an average of 125 officers per site. Other changes that can be found at every nuclear plant include physical improvements to provide additional protection against vehicle bombs, as well as additional protective measures against water- and land-based assaults. Every plant has increased security patrols, augmented security forces, added more security posts, increased vehicle standoff distances, tightened access controls, and enhanced coordination with state and local law enforcement.

NEI calculates that the collective cost of this additional security since September 2001 totals over $1 billion. The physical improvements and equipment upgrades comprise the majority of this total, yet the industry also has spent hundreds of millions of dollars on additional personnel. NRC security spending has also increased and, as the industry funds 90 percent of the NRC's budget through user fees, the industry has paid more than $70 million to fund the additional security efforts of its regulator.

INDUSTRY HAS COMMISSIONED MAJOR STUDIES EXAMINING NUCLEAR PLANT ABILITY TO WITHSTAND ATTACK

In early 2002, NEI asked EPRI—a nonprofit energy research institute—to analyze whether nuclear power plant structures that house nuclear fuel could withstand an intentional aircraft impact, like those of Sept. 11. Aircraft impact issues have been addressed in the licensing process for all 103 operating reactors, but those evaluations were conducted on the basis that the crash would be accidental. EPRI's independent study was conducted by experts in impact analysis related to commercial and military applications. Their results were peer-reviewed by an expert in the dynamic analysis of structures and a renowned structural analyst.

The EPRI study found nuclear power plant containment buildings and used fuel storage pools would protect reactor fuel even if the structures were struck by a fully loaded Boeing 767-400 flying at approximately the same speed as the airplane that crashed into the Pentagon. The study also found that such an impact would not breach the used fuel storage containers used at many plants to store used nuclear fuel outside a used fuel pool. Such a crash certainly would cause a significant amount of collateral plant damage, and no doubt would shut down the plant. However, the EPRI study concluded that such an event would not cause a release of radiation, because it would not breach reactor containment, nor would it cause the spent fuel pool to lose the cooling water that shields the fuel from the environment.

NEI also conducted a hypothetical study to determine the risk to public safety from a release of radiation assumed by a successful terrorist ground assault on a nuclear power plant. This study found that the risk to the public from a core damage accident caused by an armed terrorist ground attack on a commercial nuclear power plant is small. It is comparable to, or less than, the risk from other types of accidents postulated for U.S. commercial nuclear plants.

It is unlikely that a ground assault terrorist attack could successfully cause damage to a nuclear reactor because of plant owner capabilities to detect insider activities, physically deter attackers and mitigate accidents with operator actions and safety systems. The likelihood of severe release of radiation due to a damaged reactor is even lower, owing to the inherent strength of containment and radioactivity removal capabilities of containment and systems design. In other words, terrorists would not only need to overwhelm a plant's security forces, take over the plant and contend with an off-site response from local government authorities, they would need to figure out how to defeat primary and secondary shutdown systems and cause a reactor meltdown. Even then, they would still need to determine how to create a breach in a reinforced concrete containment building in order to achieve a radioactive release that could possibly reach the public.

Even if core damage and radiological release occur, our study also found that the public health consequences would not be catastrophic. The mean number of prompt fatalities is estimated at two people, and the mean number of latent cancer fatalities is estimated at less than 100, which is indistinguishable from cancer fatality risks from all causes within the population. For a terrorist group, determining another target instead of a nuclear plant that could be attacked with a greater likelihood of success and a much greater loss of life is not a difficult task.

It is our goal to make commercial nuclear power plants very unattractive targets for a terrorist group intent on causing loss of life. Our exceptionally strong structures and added security measures make a successful terrorist attack, even from the air, exceedingly unlikely. As shown by these studies, the chances that even a successful attack would actually cause a loss of life, other than from the attack itself, are also remarkably low, further reducing the likelihood that a terrorist would choose a nuclear power plant as a target. This is the case now, and we are committed to keeping it that way.

TREATMENT OF SECURITY THREATS BEYOND REGULATORY LIMITS

When the NRC issued the new DBT in April 2003, it stated that security at nuclear power plants had been taken to the limit of what licensees can be expected to provide. The industry is fully committed to constantly maintaining and improving plant security as necessary, yet it agrees with the NRC assessment. We have taken industrial security to, and perhaps beyond, its logical limit. At some point, postulated threats, such as attacks by military-sized forces or by forces using advanced weaponry, are the responsibility of the federal government. Privately funded security forces have practical as well as legal limits on the force they can use and thus on their overall capabilities to defend against an attack.

The industry has supported several provisions that would clarify plant security officers' ability to use certain weaponry, as well as their ability to use deadly force. Clarifying these issues would help better define the roles and responsibilities of private entities and the government in providing security at our plants.

The industry has responded to concerns that there may be attacks beyond the capabilities of the security provided by the plant by coordinating its security efforts with local, state and federal governments. Although such coordination existed prior to Sept. 11, it has been substantially increased and made part of our overall security strategy. The industry has been coordinating with DHS and with state security directors to assure that its security is adequately assisted in the unlikely event of a terrorist attack.

The industry recently established a Nuclear Sector Coordinating Committee (NSCC) with DHS to provide a forum for integrating on-site and off-site resources for threats that exceed our stand-alone capabilities. The industry is fully committed to working with all levels of government in providing the best security possible to deter an attack and to provide the best possible response should one occur.

The industry stands ready to work with federal agencies engaged in homeland defense to share its lessons learned and to provide insights into the role of commercial entities in protecting our critical infrastructure.

FORCE-ON-FORCE EXERCISES HAVE BEEN SIGNIFICANTLY IMPROVED

The industry has not only been improving its security, but has also been working to improve the testing of that security. Prior to Sept. 11, 2001, the NRC operated a program that ensured each plant had an adequate strategy for responding to the DBT with force-on-force drills. These drills were conducted at each plant roughly every eight years. The NRC's program prior to Sept. 11 had been criticized by outside groups for their adequacy in testing security and by the industry for a lack of consistency.

Although we do not consider a ground assault a likely mode of attack at a nuclear power plant, it is the only mode than can be tested with a force-on-force exercise that simulates an actual attack. As a result, it is important that these exercises are as realistic as possible and that they are

measured against a consistent set of performance standards. The new program is a rigorous and systematic approach that addresses each of these issues.

Each plant will now be testing its security multiple times each year. One of these drills at least once every three years will be evaluated by the NRC. The NRC has established standards for the qualifications of the adversary forces that participate in the force-on-force drills. Licensees must also conduct a similar test of each security shift once per year. The NRC also will take a more active role in each drill by reviewing the overall plan as well as viewing the drills at each plant. In this manner, the NRC can assure that its high standards are met.

The NRC also has established requirements for the capabilities and qualifications of our security forces. To avoid fatigue, the NRC has imposed limitations on the number of work hours of our security personnel.

The primary purpose of the force-on-force exercise is to test the defensive capabilities of the plant; however, an effective exercise hinges on the capabilities of the adversaries as well. To this end, the industry has established a Composite Adversary Force that is skilled in offensive tactics and has the training and qualifications to meet the NRC standard. This force will consist of full-time, highly trained, security experts. The adversary force will be used in the triennial NRC-evaluated exercises and will thus present a state-of-the-art challenge to our plants. In addition to evaluating the defensive capabilities of the plant, the NRC also will evaluate the adversary force to ensure a robust exercise. Through this program, assurance is further provided that our security forces can successfully respond to a dedicated adversary team.

We are unaware of any security forces for any private industry that are subjected to such rigorous testing that includes force-on-force drills using a full-time dedicated team.

NUCLEAR PLANT SECURITY, PRAISED BY INDEPENDENT EXPERTS AND SOURCES

Objective reviews from unbiased sources have almost uniformly praised our security as the best or among the best of any industrial sector. The industry's security has been recognized as excellent in independent assessments conducted by the Progressive Policy Institute, a panel of security and 14 infrastructure experts for The Washington Post, and by current and former law enforcement officials.

The Progressive Policy Institute, in a report on homeland security issued last summer, gave nuclear plant security its only "A" rating. When The Washington Post reviewed security in several U.S. private and government sectors a year after Sept. 11, a panel of experts gave the nuclear industry a rating of "A-/B+"—the second-highest rating in the survey. More recently, the National Journal, in a bipartisan survey, gave nuclear plant security its third-highest ranking.

The industry does have its critics, however. The Union of Concerned Scientists released a report last week that postulates a series of worst-case scenarios resulting from a terrorist attack. Riverkeeper, an advocacy group opposed to Indian Point, commissioned the report. Ed Lyman, the author of the report, purports to analyze the consequences of a radiation release resulting

from such an attack and dismisses the NRC assessments regarding the low probability of this type of event.

A team of industry technical analysts, including representatives from the Palo Alto, Calif.-based research institute EPRI, found that the report "is based on bad science masquerading as a complex analysis" and that it applied data from various sources "in a manner that is both unrealistic and inappropriate." The team also noted that the report fails to take into account the extremely low probability of a commercial aircraft's penetrating a plant containment wall, damaging plant components and the reactor within. Without taking into account such a low-probability event, the report's "analysis is worthless."

Still, advocacy groups long opposed to nuclear energy continue to compile "reports" projecting catastrophic consequences of a potential terrorist attack, painting pictures of hugely implausible scenarios. This report, and other such studies, should be considered in light of realistic and rational assumptions.

NUCLEAR INDUSTRY SUPPORTS NUCLEAR SECURITY LEGISLATION

The nuclear industry supports several legislative proposals from the NRC that would enhance its security efforts. The Energy and Commerce Committee of the House of Representatives considered and passed several of these proposals in 2003. The Senate Environment and Public Works Committee also has considered and passed several security proposals. The proposals include increasing the penalties for sabotage of a nuclear facility and making it a federal crime to bring an unauthorized weapon into one of our facilities. Although not included in these bills, the industry supports efforts to clarify the weaponry that can be used by our security forces, as well as their ability to use deadly force.

These proposals were the subject of the energy bill conference and many are now included in the energy bill conference report pending before Congress. The industry does not agree with every aspect of the proposals; however, it has supported passage of the energy bill, including the nuclear plant security provisions.

POLICY IMPLICATIONS OF INCREASING NUCLEAR PLANT SECURITY REQUIREMENTS

The nuclear energy industry urges Congress and other policymakers to take into account the NRC's view that nuclear power plant security has been raised to a private entity's limits. The industry agrees with this assessment. The determination of what is—and is not—a responsible level of overall security for our nation's critical infrastructure is largely the purview of our government, not private industry. If Congress or the administration believes that protection against larger or more serious threats is necessary, then the industry urges consideration of the practical limits of what a commercial entity can and should offer. At some point, industrial security becomes national security.

The nuclear energy industry also urges Congress and other policymakers to consider greater policy implications arising from extensive security being provided at our plants. This security is top-rate and top-dollar. Nuclear power provides enormous benefits to our economy, our national

security and our environment. Security at our plants must be more than adequate, but not an unnecessary burden that only the nuclear energy industry must carry.

Finally, the nuclear industry urges Congress and other policymakers to consider whether resources are being properly utilized. The nuclear energy industry has responded effectively and rapidly to improve its security after Sept. 11, 2001. But, much of this response is attributable to the existence of a federal regulator, the NRC, with the ability to impose and enforce new security mandates. As such, the nuclear energy industry's security requirements have dramatically exceeded those for any other major industrial sector—including industries that do not have a regulator with authority similar to the NRC's. A rational homeland security policy identifies targets based upon risk and allocates resources appropriately. Risk assessments by notable security authorities have found—based on past terrorist targets—that nuclear plants are hardened targets and are considerably less likely to be the focus of terrorist attacks.

In summary, our defenses were exceptional prior to Sept. 11, and they are even better today. It is highly unlikely that attackers could successfully breach security at a nuclear power plant and even more unlikely they could produce a release of radiation that would endanger the residents near the plant. In addition, security at our nuclear power plants is not static. We are constantly reviewing and reevaluating our security programs. Consequently, America's nuclear energy industry will continue to play its role as a leader and model for protecting our country's critical infrastructure.

FACT SHEET

Nuclear Power Plant Security

September 2004

NEI
NUCLEAR ENERGY INSTITUTE

SUITE 400
1776 I STREET, NW
WASHINGTON, DC
20006-3708
202.739.8000
www.nei.org

Key Facts

■ The defense-in-depth philosophy used in the construction and operation of nuclear power plants provides high levels of protection for public health and safety.

■ The Nuclear Regulatory Commission has always imposed on nuclear power plants the highest security standards of any American industry. The industry meets or exceeds these requirements in all areas. All commercial nuclear power plants have well-armed and highly trained security forces—some 8,000 officers—that are routinely drilled and tested.

■ Since Sept. 11, 2001, security has been significantly strengthened. The NRC in February 2002 and again in April 2003 ordered enhanced security by the industry.

■ The industry has added about 3,000 officers and upgraded physical security over the past three years. The industry has spent an additional $1 billion on security since September 2001.

■ Access to nuclear power plants, tightened since Sept. 11, is controlled by a physical barrier system and security officers who search all entering vehicles and people. All workers entering plant operating areas also must pass through sensitive metal and explosives detection equipment.

■ Plant operators also have installed additional vehicle barrier systems to protect against vehicle bombs.

■ The industry coordinates with the NRC, Department of Homeland Security and intelligence agencies on the assessment of potential threats and the specific actions by industry security forces in the event of a credible threat against a commercial nuclear facility.

■ All commercial nuclear plants have emergency response procedures and contingency plans in the event of a plant accident or terrorist event. These procedures, reviewed and improved following Sept. 11, are evaluated every two years during extensive drills involving plant personnel and local police, fire and emergency management organizations. NRC and Federal Emergency Management Agency (FEMA) expert teams evaluate these drills.

Plant Security Meets All Federal Requirements

The nuclear energy industry is one of the few whose security program is regulated by the federal government. The NRC's requirements for nuclear power plant security are predicated on the need to protect the public from the possibility of exposure to radioactive releases caused by acts of sabotage. Intelligence information and incidents around the world are analyzed to ensure plant protection regulations are updated to reflect potential threats.

The NRC's security regulations are designed to ensure that the industry's security force can protect against specific ground-based threats. The threat against which the industry must defend is characterized as a suicidal, well-trained paramilitary force, armed with automatic weapons and explosives, and intent on forcing its way into a nuclear power plant to commit radiological sabotage. Such a force may have the assistance of an "insider," who could pass along information and help the attackers. The presumed goal of such an attack would be the release of radioactive material from the plant.

The NRC's "design basis threat" provides a foundation for developing defensive

Nuclear Power Plant Security

response strategies that cover a variety of situations. The NRC bases the design basis threat on technical studies and information received from intelligence experts and federal law enforcement agencies. It is reviewed by the agency twice a year.

Over the past three years, the NRC has twice raised the threat level against which nuclear plants must provide protection. In doing so, the NRC has assumed an increased number of possible attackers and weapons capabilities.

Many industry security elements are considered "safeguards" information, which means they are controlled on a "need-to-know" basis. Clearly, plant protection capabilities and response strategy should be controlled and protected from public disclosure to avoid compromises that might benefit a potential adversary.

Defense-in-Depth Against Potential Threats

The FBI considers security forces and infrastructure at nuclear power plants formidable and considers nuclear power plants difficult to penetrate.

In addition, the defense-in-depth features that protect the public from radiological hazard in the event of a reactor incident also protect the plant's fuel and related safety systems from attempted sabotage. The design of each plant emphasizes the reliability of plant systems, redundancy and diversity of key safety systems, and other safety features to prevent incidents that could pose a threat to public health and safety.

Steel-reinforced concrete containment structures protect the reactor. Redundant safety and reactor shutdown systems have been designed to withstand the impact of earthquakes, hurricanes, tornadoes and floods. Areas of the plant that house the reactor and used reactor fuel also would withstand the impact of a widebody commercial aircraft, according to peer-reviewed analyses by EPRI, a Palo Alto, Calif.-based research organization. Operations personnel are trained in emergency procedures that would be used to keep the plant safe from a sabotage attempt.

A two-day national security exercise conducted by the Center for Strategic and International Studies in 2002 found that nuclear power plants would be less attractive targets to terrorist organizations because of the industry's robust security program. The exercise was designed to explore difficulties and reveal vulnerabilities that might arise if the nation were faced with a credible, but ambiguous, threat of a terrorist attack on American soil.

"Silent Vector" was developed and produced by CSIS in partnership with the ANSER Institute for Homeland Security and the Oklahoma City National Memorial Institute for the Prevention of Terrorism. Potential targets included refineries, large liquefied natural gas or liquefied petroleum gas storage operations, pipeline infrastructure, petroleum terminals, nuclear power plants, chemical operations and dams.

CSIS President John Hamre said that nuclear power plants "are probably our best-defended targets. There is more security around nuclear power plants than anything else we've got ... One of the things that we have clearly found in this exercise is that this is an industry that has taken security pretty seriously for quite a long time, and its infrastructure, especially against these kinds of terrorist threats, is extremely good."

David McIntyre, former deputy director of the ANSER Institute for Homeland Security, added that "during the eight months of research that went into this, there were some issues like that [communication and coordination] that turned out not to be as great as we thought. And the nuclear industry was one of those that turned out to be much better connected—much more progressive, frankly—than I'd anticipated when we began the research."

Security Increased Since Sept. 11, 2001

Immediately after the events of Sept. 11, 2001, security at every nuclear power plant was placed on its highest level. Nuclear plant security now is consistent with Homeland Security threat levels.

Nuclear Power Plant Security

As a result, access to the plants is more strictly controlled; the defensive perimeters have been extended and reinforced, and security forces and capabilities have been augmented. Further, coordination with law enforcement, the intelligence community and the military has been enhanced. At some plants, these efforts have been supplemented by National Guard, U.S. Coast Guard, state police or other forces.

In February 2002, the NRC formalized many of the enhancements to security that the industry had already implemented. The agency subsequently issued new requirements further restricting access authorization.

In April 2003, the NRC issued rules limiting the working hours of security personnel and requiring increased training including weapons proficiency. All U.S. nuclear power plants submitted plans for meeting the NRC's additional security requirements relating to working hours, training and other areas in April 2004. They will implement these plans by October 2004.

Site Security Measures. All commercial nuclear plants have established extensive security measures. Plant operators and the NRC inspect these measures and test them in drills to uncover any vulnerability. Security measures include:

- physical barriers and illuminated detection zones
- approximately 8,000 well-trained and well-equipped armed security officers at 64 sites
- surveillance and patrols of the perimeter fence
- intrusion detection aids (including several types of detection fields, closed-circuit television systems and alarm/alert devices)
- bullet-resisting barriers to critical areas
- a dedicated contingency response force.

All threats will be countered with dedicated, tactically trained, well-armed security officers who collectively determine the nature of a threat, assess its magnitude and take aggressive steps to deter the threat.

Controlled Access. Access to a nuclear power plant requires passage through a larger "owner-controlled area" surrounding the plant. Access to specific parts of the plant is controlled by physical barriers and security officers.

Access to an interior fenced area—the protected area, where the reactor building is located—is controlled by security officers and physical barriers. Vehicle barriers and/or other physical boundaries ensure that the protected area of the plant cannot be breached by a direct vehicular assault or by detonation of a vehicle bomb. All vehicles, personnel and material entering the protected area first must be thoroughly inspected by security officers to ensure that no weapons, explosives or other such items are brought onto the plant site.

Access to the "protected area" of the plant is controlled through the use of physical barriers, intrusion detection equipment, closed-circuit surveillance equipment, a designated isolation zone and exterior lighting. Access to the inner areas of the plant where vital equipment is located also is controlled through the use of physical barriers, locked and alarmed doors, and card-reader or hand geometry access control systems.

The barriers are substantial enough to effectively delay entry in order to allow for an effective armed response by plant security forces. Within the protected zone, access to all vital areas of the plant is even more secure. This access may be controlled by a security officer or provided by computer-controlled "key-card" access systems. Plant employees must have a documented need prior to gaining access to each vital area, and their movements are tracked by key-card access points throughout the vital area.

Reactor Operators Act in Concert With Security. Reactor operators train frequently to be sure they can respond to a range of unusual events. Plant operators have emergency procedures in place specifically for security situations, including automatic shutdown of the

Nuclear Power Plant Security

reactor in the event of an attack. Emergency planning and public notification systems support protection of public health and safety. The NRC periodically evaluates these plans during exercises or drills, which may also involve local police, fire and emergency management organizations.

Protecting Against An Insider Threat

All nuclear power plants have programs that reduce the potential for threats from plant personnel, or "insiders." These include authorization criteria for those allowed unescorted access to the plant's protected area and "fitness-for-duty" programs to deter drug and alcohol abuse.

Strong behavioral observation programs are in place requiring personnel to be trained to observe and report behavior that may be a potential threat to the normal operation of a nuclear power plant. In addition, many companies provide teamwork development programs that promote commitment and accountability in the work force.

Access Authorization. Before new nuclear plant employees or contractor employees are allowed unescorted access to the protected area, they must pass several tests and background checks to determine whether they are trustworthy and reliable. These tests include drug and alcohol screening, psychological evaluations, plus a check with former employers, education records, criminal histories (through the FBI) and credit histories.

Fitness-for-Duty Programs. Companies that operate nuclear power plants demand and ensure that personnel perform their duties in a safe, reliable and trustworthy manner, and are not under the influence of legal or illegal substances, or mentally or physically impaired from other causes, that would adversely hinder their ability to competently perform their duties. Employees who have unescorted access to the plant's protected area must maintain their fitness-for-duty. The NRC requires companies to conduct random drug and alcohol testing on their employees. As a result, at least half of all employees are tested annually.

Behavioral Observation. Employees with unescorted plant access are subject to continual behavioral observation programs. Behavioral observation is conducted by all personnel who have been trained in behavioral observation. Behavioral observation is designed to detect individual behavioral changes, which, if left unattended, could lead to acts detrimental to public safety. Employees are offered counseling if they have job performance problems or exhibit unusual behavior. Similarly, anyone who appears to be under the influence of drugs or alcohol is immediately removed from the work area for evaluation.

This fact sheet is also available at www.nei.org, *where it is updated periodically.*

FACT SHEET

Post-Sept. 11 Improvements in Nuclear Plant Security Set U.S. Industry Standard

August 2004

NEI
NUCLEAR ENERGY INSTITUTE

SUITE 400
1776 I STREET, NW
WASHINGTON, DC
20006-3708
202.739.8000
www.nei.org

Key Facts

- Nuclear plants are the most secure facilities in the U.S. industrial infrastructure.
- The nuclear energy industry, working with the Nuclear Regulatory Commission, has implemented additional security measures at nuclear facilities since Sept. 11, 2001.
- Recent studies and exercises have confirmed that nuclear facilities are well defended and difficult for terrorists to penetrate.

Setting the Standard for Industrial Security

The nuclear industry responded quickly and effectively to the events of Sept. 11. Security at nuclear plants, already the most secure facilities in the U.S. industrial infrastructure, was bolstered and has remained at a heightened level of alert.

Security forces at nuclear plants were increased by 33 percent to approximately 7,000 officers at 67 sites. By the end of 2004, the industry will have spent an additional $1 billion in security-related improvements since September 2001.

In 2001, the industry averaged $5 million per site on security-related expenditures. Security expenditures increased to $7.3 million per site in 2003.

The industry, working with the NRC, instituted additional security measures since Sept. 11, such as:

- extending and fortifying security perimeters
- increasing patrols within security zones
- installing new barriers to protect against vehicle bombs
- installing additional high-tech surveillance equipment
- strengthening coordination of security efforts with local, state and federal agencies to integrate approaches among the entities—a position the industry continues to support.

In February 2002, the NRC formalized many of the security enhancements that the industry had implemented since Sept. 11. The NRC has enhanced its requirements to further restrict access at nuclear plants.

In April 2003, the NRC issued new orders that limit the hours security personnel may work each week. In addition, the NRC increased the training requirements for nuclear plant security officers, including training in weapons proficiency.

Since Sept. 11, the NRC has twice significantly increased the definition of the threat against which nuclear plants must provide protection. As a result, nuclear plants now are able to defend against a greater number of attackers, armed with more weapons than ever before.

Working with the NRC, the industry continues to examine ways to improve security at all U.S. nuclear facilities at every level.

Studies Confirm Strength Of Nuclear Plant Security

A two-day national security exercise conducted by the Center for Strategic and International Studies (CSIS) in 2002 found that nuclear plants would be less attractive than other potential targets to terrorist organizations because of the industry's robust security programs. The exercise was

Post-Sept. 11 Improvements in Nuclear Plant Security Set U.S. Industry Standard

designed to explore difficulties and reveal vulnerabilities that might arise in the event of a credible, but ambiguous, threat of a terrorist attack on American soil.

At the conclusion of the exercise, CSIS President John Hamre said that nuclear power plants "are probably our best-defended targets. There is more security around nuclear power plants than anything else we've got."

Peer-reviewed analyses conducted by EPRI, a Palo Alto, Calif.-based research firm, revealed that structures that house the reactor and nuclear fuel facilities would be protected against a release of radiation even if struck by a large commercial jetliner.

State-of-the-art computer modeling techniques determined that typical nuclear plant containment structures used fuel storage pools, fuel storage containers and used fuel transportation containers would withstand a potential impact despite some concrete crushing and bent steel. In all cases, public security would be protected.

More information on NRC security initiatives since Sept. 11 is available at www.nrc.gov.

This fact sheet is also available at www.nei.org, *where it is updated periodically.*

CHERNOBYL ON THE HUDSON?

THE HEALTH AND ECONOMIC IMPACTS OF A TERRORIST ATTACK AT THE INDIAN POINT NUCLEAR PLANT

Edwin S. Lyman, PhD
Union of Concerned Scientists
September 2004

Commissioned by Riverkeeper, Inc.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 4
INTRODUCTION 7
(a) The terrorist threat to nuclear power plants 7
(b) The Nuclear Regulatory Commission: an agency in denial 8
(c) The CRAC2 Report 12
ACCIDENTS: DESIGN-BASIS, BEYOND-DESIGN-BASIS, AND DELIBERATE .. 19
(a) Design-basis accidents 19
(b) Beyond-design-basis accidents 19
(c) "Deliberate accidents" 21
THE HEALTH CONSEQUENCES OF A RADIOLOGICAL RELEASE FROM INDIAN POINT 23
THE MACCS2 CODE 26
THE SABOTAGE SCENARIO 28
(a) The source term 28
(b) Meteorology 33
(c) Protective actions 35
(d) Population distribution 36
RESULTS 38
(a) Consequences of radiological exposures during "emergency phase" 39
(b) Doses received by individuals outside of the 10-mile EPZ 42
(i) Thyroid doses to children, their consequences, and the need for KI distribution 42
(ii) Whole-body doses and the need for evacuation or sheltering 47
(c) Long-term economic and health consequences 49
(i) EPA Protective Action Guide cleanup standard 49
(ii) Relaxed cleanup standard 51
(d) An even worse case 52
CONCLUSIONS 54
ACKNOWLEDGMENTS 54

TABLES

TABLE 1: NUREG-1465 radionuclide releases into containment for PWRs 31
TABLE 2: Source term used in MACCS2 model 33
TABLE 3: Terrorist attack at IP 2, MACCS2 estimates of early fatalities (EFs), latent cancer fatalities (LCFs) and the EF distance resulting from emergency phase exposures, 100% evacuation of EPZ 40
TABLE 4: Terrorist attack at IP 2, MACCS2 estimates of early fatalities (EFs), latent cancer fatalities (LCFs) and the EF distance resulting from emergency phase exposures, 24-hour sheltering in EPZ 40
TABLE 5: Terrorist attack at IP 2, MACCS2 estimates of early fatalities (EFs), latent cancer fatalities (LCFs) and the EF distance resulting from emergency phase exposures, normal activity in EPZ 41
TABLE 6: Terrorist attack at IP 2, MACCS2 estimates of centerline thyroid doses to 5-year-olds resulting from emergency phase exposures (all doses in rem) 44
TABLE 7: Terrorist attack at IP 2, MACCS2 estimates of adult centerline whole-body total effective dose equivalents (TEDEs) resulting from emergency phase exposures (all doses in rem) 48
TABLE 8: Terrorist attack at IP 2, MACCS2 95th percentile estimates of early fatalities (EFs) and latent cancer fatalities (LCFs) resulting from emergency phase exposures; 25-mile EPZ 48
TABLE 9: Terrorist attack at IP 2, MACCS2 estimates of long-term economic and health consequences, EPA intermediate phase PAG (< 2 rem in first year; approx. 5 rem in 50 yrs) 51
TABLE 10: Long-term economic and health consequences of a terrorist attack at IP 2, relaxed cleanup standard (25 rem in 50 years) 52
TABLE 11: Terrorist attack at IP 2 and 3, MACCS2 estimates of early fatalities (EFs) and latent cancer fatalities (LCFs) resulting from emergency phase exposures, 100% evacuation of EPZ 53

EXECUTIVE SUMMARY

Since 9/11, the specter of a terrorist attack at the Indian Point nuclear power plant, thirty-five miles upwind from midtown Manhattan, has caused great concern for residents of the New York metropolitan area. Although the Nuclear Regulatory Commission (NRC) ordered modest security upgrades at Indian Point and other nuclear power plants in response to the 9/11 attacks, the plants remain vulnerable, both to air attacks and to ground assaults by large terrorist teams with paramilitary training and advanced weaponry. Many question whether the NRC's security and emergency planning requirements at Indian Point are adequate, given its attractiveness as a terrorist target and the grave consequences for the region of a successful attack.

This report presents the results of an independent analysis of the health and economic impacts of a terrorist attack at Indian Point that results in a core meltdown and a large radiological release to the environment. We find that, depending on the weather conditions, an attack could result in as many as 44,000 near-term deaths from acute radiation syndrome or as many as 518,000 long-term deaths from cancer among individuals within fifty miles of the plant. These findings confirm that Indian Point poses a severe threat to the entire New York metropolitan area. The scope of emergency planning measures should be promptly expanded to provide some protection from the fallout from an attack at Indian Point to those New York area residents who currently have none. Security at Indian Point should also be upgraded to a level commensurate with the threat it poses to the region.

A 1982 study by Sandia National Laboratories found that a core meltdown and radiological release at one of the two operating Indian Point reactors could cause 50,000 near-term deaths from acute radiation syndrome and 14,000 long-term deaths from cancer. When these results were originally disclosed to the press, an NRC official tried to reassure the public by saying that the kind of accident the study considered would be less likely than "a jumbo jet crashing into a football stadium during the Superbowl."

In the post-9/11 era, the possibility of a jumbo jet crashing into the Superbowl --- or even a nuclear power plant --- no longer seems as remote as it did in 1982. Nonetheless, NRC continues to argue that the 1982 Sandia report is unrealistic because it focused on "worst-case" accidents involving the simultaneous failure of multiple safety systems, which are highly unlikely to occur by chance. But when the potential for terrorist attacks is considered, this argument no longer applies. "Worst-case" scenarios are precisely the ones that terrorists have in mind when planning attacks.

Both NRC and Entergy, the owner of Indian Point, assert that even for the most severe terrorist attack, current emergency plans will be adequate to protect residents who live in the evacuation zone within 10 miles of the plant. They also say that there will be no significant radiological impact on New York City or any other location outside of the 10-mile zone. Accordingly, NRC has opposed proposals made after 9/11 to extend the emergency planning zone around Indian Point. However, NRC and Entergy have not

provided the public with any documentation of the assumptions and calculations underlying these claims.

In view of the lack of public information available on these controversial issues, we carried out an independent technical analysis to help inform the debate. Our calculations were performed with the same state-of-the-art computer code that NRC uses to assess accident consequences. We used the NRC's guidance on the radiological release from a core meltdown, current estimates of radiation risk, population data from the 2000 census, and the most recent evacuation time estimate for the 10-mile Indian Point emergency planning zone. Following the format of the 1982 Sandia report, we calculated the numbers of near-term deaths from acute radiation syndrome, the numbers of long-term deaths from cancer, and the maximum distance at which near-term deaths can occur. We evaluated the impact of both evacuation and sheltering on these outcomes. We also estimated the economic damages due to the long-term relocation of individuals from contaminated areas, and the cost of cleanup or condemnation of those areas.

The health and environmental impacts of a large radiological release at Indian Point depend strongly on the weather conditions. We have carried out calculations for over 140,000 combinations of weather conditions for the New York area and wind directions for the Indian Point site, based on a year's worth of weather data. For this data set, we have determined the average consequences, the peak consequences, and the consequences for "95th percentile" weather conditions (in other words, only 5% of the weather sequences analyzed resulted in greater consequences).

We believe that the 95th percentile results, rather than the average values, represent a reasonable assessment of the likely outcome of a successful terrorist attack, since such attacks would most likely not occur at random, but would be timed to coincide with weather conditions that favor greater casualties. Attacks capable of causing the peak consequences that we calculate would be difficult to achieve because of inaccuracies in weather forecasts, restricted windows of opportunity and other factors, but remain within the realm of possibility.

For a successful attack at one of the two operating Indian Point reactors, we find that

- The number of near-term deaths within 50 miles, due to lethal radiation exposures received within 7 days after the attack, is approximately 3,500 for 95th percentile weather conditions, and approximately 44,000 for the worst case evaluated. Although we assumed that the 10-mile emergency planning zone was entirely evacuated in these cases, this effort was inadequate because (according to Entergy's own estimate) it would take nearly 9.5 hours to fully evacuate the 10-mile zone, whereas in our model the first radiological release occurs about two hours after the attack.

- Near-term deaths can occur among individuals living as far as 18 miles from Indian Point for the 95th percentile case, and as far as 60 miles away in the worst case evaluated. Timely sheltering could be effective in reducing the number of

near-term deaths among people residing outside of the 10-mile emergency planning zone, but currently no formal emergency plan is required for these individuals.

- The number of long-term cancer deaths within 50 miles, due to non-acutely lethal radiation exposures within 7 days after the attack, is almost 100,000 for 95th percentile weather conditions and more than 500,000 for the worst weather case evaluated. The peak value corresponds to an attack timed to coincide with weather conditions that maximize radioactive fallout over New York City.

- Based on the 95th percentile case, Food and Drug Administration guidance would recommend that many New York City residents under 40, and children in particular, take potassium iodide (KI) to block absorption for radioactive iodine in the thyroid. However, there is no requirement that KI be stockpiled for use in New York City.

- The economic damages within 100 miles would exceed $1.1 trillion for the 95th percentile case, and could be as great as $2.1 trillion for the worst case evaluated, based on Environmental Protection Agency guidance for population relocation and cleanup. Millions of people would require permanent relocation.

We hope that this information will be useful to Federal, State and local homeland security officials as they continue to develop plans to protect all those at risk from terrorist attacks in the post-9/11 world.

INTRODUCTION

(a) The terrorist threat to nuclear power plants

Public concern about the vulnerability of nuclear power plants to catastrophic acts of sabotage soared in the aftermath of the September 11 terrorist attacks. There is ample justification for this concern.

Soon after the 9/11 attacks, the Nuclear Regulatory Commission conceded that U.S. nuclear power plants were not designed to withstand the high-speed impact of a fully fueled, modern passenger jet. The report of the 9/11 Commission has revealed that al Qaeda considered attacks on nuclear plants as part of their original plan, but declined to do so primarily because of their mistaken belief that the airspace around nuclear power plants in the U.S. was "restricted," and that planes that violated this airspace would likely be shot down before impact.[1]

But al Qaeda is surely now aware that no such restrictions were in place on 9/11. And it is clear from press reports that even today, no-fly zones around nuclear plants are imposed only at times of elevated threat level, and are limited in scope to minimize their economic impact on the aviation industry. This policy reflects a confidence in the ability of the intelligence community to provide timely advance warning of a surprise attack that --- given the 9/11 example --- is not entirely warranted. Moreover, even when no-fly zones are in place around nuclear plants, they are not likely to be effectively enforced. For instance, the U.S. government does not require that surface-to-air anti-aircraft protection be provided at nuclear plants, although such defenses have been routinely employed in Washington, D.C. since the 9/11 attacks.

In addition to the aircraft threat, many have begun to question the adequacy of physical security at nuclear plants to protect against ground-based, paramilitary assaults, in view of revelations that thousands of individuals received sophisticated training in military tactics at al Qaeda camps in Afghanistan. Press reports have documented many security failures at nuclear plants around the country, and have called attention to the troubling statistic that during a series of security performance tests in the 1990s, guard forces at nearly 50% of US plants failed to prevent mock terrorist teams from simulating damage that would have caused meltdowns had they been real attacks. This information, which was widely available but largely ignored before 9/11, suddenly became far more alarming in the new threat environment.

Today, the danger of a terrorist attack at a nuclear power plant in the United States --- either from the air or from the ground --- is apparently as great as ever. According to a January 14, 2004 speech by Robert L. Hutchings, Chairman of the National Intelligence Council (NIC),[2]

---

[1] *The 9/11 Commission Report, Authorized Edition*, W.W. Norton, New York, 2004, p. 245.
[2] Robert L. Hutchings, "Terrorism and Economic Security," speech to the International Security Management Organization, Scottsdale, AZ, January 14, 2004.

> "targets such as nuclear power plants ... are high on al Qa'ida's targeting list as a way to sow panic and hurt our economy ... The group has continued to hone its use of transportation assets as weapons ... although we have disrupted several airline plots, we have not eliminated the threat to airplanes. There are still al Qa'ida operatives who we believe have been deployed to hijack planes and fly them into key targets ... Al Qa'ida's intent is clear. Its capabilities are circumscribed but still substantial. And our vulnerabilities are still great."

More recently, the 9/11 Commission concluded that "major vulnerabilities still exist in cargo and general aviation security. These, together with inadequate screening and access controls, continue to present aviation security challenges."[3]

(b) The Nuclear Regulatory Commission: an agency in denial

Since 9/11, members of the public, non-profit groups and lawmakers across the United States have been calling for major security upgrades at nuclear power plants, including consideration of measures such as military protection against ground assault and anti-aircraft defenses against jet attack. Yet the response of the Nuclear Regulatory Commission (NRC), the agency that regulates both the safety and security of US nuclear reactors, has not been commensurate with the magnitude of the threat.[4] And the Department of Homeland Security, the agency charged with coordinating the defense of the entire US critical infrastructure against terrorist attacks, appears to be merely following NRC's lead.[5]

Notwithstanding a steady stream of FBI warnings citing nuclear power plants as potential terrorist targets, NRC continues to maintain that there is no need to consider measures that could reduce the vulnerability of nuclear plants to air attack. NRC's position is that "the best approach to dealing with threats from aircraft is through strengthening airport and airline security measures."[6]

As it became clear that NRC was not going to require the nuclear industry to protect nuclear plants from attacks on the scale of September 11, some groups began calling for plants to be shut permanently. Because many of the most dangerous fission products in a nuclear reactor core decay rapidly after shutdown, the health consequences of a terrorist attack on a shutdown nuclear reactor would be significantly lower than those of an attack on an operating reactor.[7]

---

[3] *9/11 Commission Report* (2004), op cit., p. 391.
[4] D. Hirsch, D. Lochbaum and E. Lyman, "NRC's Dirty Little Secret," *Bulletin of the Atomic Scientists*, May/June 2003.
[5] E. Lyman, "Nuclear Plant Protection and the Homeland Security Mandate," Proceedings of the 44th Annual Meeting of the Institute of Nuclear Materials Management, Phoenix, Arizona, July 2003.
[6] US Nuclear Regulatory Commission, "Frequently Asked Questions About NRC's Response to the 9/11/01 Events," revised March 15, 2004. On the NRC web site: http://www.nrc.gov/what-we-do/safeguards/911/faq.html#3.
[7] Calculations by the author, using the computer code MACCS2, indicate that for an attack occurring at twenty days after reactor shutdown and resulting in core melt and loss of containment, the number of early fatalities from acute radiation sickness would be reduced by 80% and the number of latent cancer fatalities

Public concern has been greatest for those plants seen as prime terrorist targets because of their symbolic importance or location near large population and commercial centers, such as the Indian Point nuclear power plant in Westchester County, New York, whose two operating reactors are situated only 24 miles from the New York City limits, 35 miles from midtown Manhattan and in close proximity to the reservoir system that supplies drinking water to nine million people. The post-9/11 movement to shut down Indian Point has attracted a level of support from the public and elected officials not seen since the early 1980s, including calls for shutdown by over 400 elected officials and over 50 municipalities.

In response to this challenge, NRC, Entergy (the owner of Indian Point), other nuclear utilities, and their trade group in Washington, the Nuclear Energy Institute (NEI), have undertaken a massive public relations campaign to assuage public fears about the risk of terrorism at Indian Point. First, they assert that a combination of robust nuclear plant design, physical security and redundant safety measures would be able to stop any terrorist attack from causing significant damage to the reactor core. Second, they argue that even if terrorists were to successfully attack Indian Point and cause a large radiological release, the public health consequences could be successfully mitigated by execution of the emergency plans already in place for residents within the 10-mile-radius "emergency planning zone" (EPZ). And third, they claim that outside of the 10-mile EPZ, exposures would be so low that no special precautions would be necessary to adequately protect the public from radiation, other than possible interdiction of contaminated produce and water.[8]

A typical example of the third argument can be found in a recent letter the NRC sent to Alex Matthiessen, Executive Director of Riverkeeper:[9]

> "Outside of 10 miles, direct exposure is expected to be sufficiently low that evacuation or sheltering would not be necessary. Exposure to a radioactive plume would not likely result in immediate or serious long-term health effects. Consideration of public sheltering and evacuation in emergency plans is very conservative and recommended at very low dose levels, well below the levels where health effects would be expected to occur."

---

resulting from lower exposures would be reduced by 50%, compared to an attack when the reactor is operating at full power. This calculation does not consider an attack on the storage pools for the highly radioactive spent fuel, which could result in significant long-term radiological contamination over a wide area and enormous economic consequences. For an extensive discussion of this threat, as well as an analysis of approaches for mitigating it, see R. Alvarez et al., "Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States," *Science and Global Security* **11** (2003) 1-51.

[8] The NRC defines two "emergency planning zones," or EPZs. The 10-mile "plume exposure" EPZ is the region where evacuation or other actions could be ordered to protect the public from coming into contact with an atmospheric release of radioactivity. The 50-mile "ingestion" EPZ is the region where interdiction of agricultural products and water supplies could be ordered to prevent the consumption of contaminated produce. No evacuation planning is required for individuals residing within the ingestion EPZ but outside of the plume exposure EPZ.

[9] Letter from Cornelius F. Holden, Jr., Office of Nuclear Reactor Regulation, US NRC, to Alex Matthiessen, Riverkeeper, September 30, 2003.

The purpose of this report is to address these three claims, with an emphasis on the second and third, by conducting a quantitative assessment of the potential consequences of a terrorist-induced radiological release at Indian Point for individuals both within and without the 10-mile EPZ, including residents of New York City.

There is a considerable need today for an independent study of these questions. At a time when the importance of rigorous emergency planning for catastrophic terrorist attacks is obvious, it is essential that responsible officials be fully apprised of the facts, especially if they contradict long-held assumptions and biases. The lives of many people could be put at jeopardy if emergency plans are not designed with the most accurate information at hand.

This means, in particular, that the emergency planning process should be designed to account for the full spectrum of potential consequences, including so-called "fast-breaking" release scenarios in which radioactive releases to the environment would begin within about thirty minutes after an attack. This was one of the major conclusions of the report carried out for the government of New York State by James Lee Witt Associates.[10] Certain terrorist attack scenarios could be capable of causing such rapid releases.

But NRC and the Federal Emergency Management Agency (FEMA) continue to be reluctant to require testing of fast-breaking radiological releases in emergency planning exercises, asserting that such events are highly unlikely to occur.[11] However, this argument is no longer relevant in an age when terrorists have acquired unprecedented levels of technical expertise, and are actively targeting critical infrastructure facilities with the intent to maximize casualties and economic damages. If current emergency plans cannot successfully cope with all credible terrorist-induced events, they should be upgraded. If upgrading to a sufficiently protective level is so cumbersome as to be practically impossible, then other options, including plant shutdown, should not be ruled out.

Members of the public deserve to be fully informed of the potential consequences for their health and property of a successful terrorist attack at Indian Point, so that they can prepare for an attack in accordance with their own judgment and willingness to accept risk. This principle is consistent with the guidance of the Department of Homeland Security, whose Web site www.ready.gov advises that "all Americans should begin a process of learning about potential threats so we are better prepared to react during an attack." Sources of technical information other than NRC and the nuclear industry are

---

[10] James Lee Witt Associates, *Review of Emergency Preparedness of Areas Adjacent to Indian Point and Millstone*, March 2003, Executive Summary, pg. x.

[11] Although it was anticipated that the widely publicized June 8, 2004 emergency planning exercise at Indian Point would involve a "fast-breaking" release, NRC in fact chose a scenario in which no release at all occurred. It was assumed that terrorists attacked the plant with a jet aircraft but missed the reactor and only managed to crash into the switchyard, causing a loss of off-site power but not enough damage to result in a radiological release. Thus the exercise provided no information as to the effectiveness of the Indian Point emergency plan in protecting residents of the EPZ from injury had the plane actually hit its target and initiated the damage scenario that is assessed in this report.

also essential to facilitate a factually accurate and honest discussion of the risks and benefits of continued operation of Indian Point in the post-9/11 era.

Some observers may criticize the public release of this report as irresponsible because they believe it (1) could assist terrorists in planning attacks, or (2) could interfere with the successful execution of emergency plans by unnecessarily frightening members of the public who the authorities claim are not at risk.

We are acutely aware of such concerns and, after careful consideration, have concluded that they do not have merit. We have reviewed this report carefully and omitted any information specific enough to be useful to terrorists seeking to attack Indian Point. Unfortunately, far more detailed information about nuclear plant design, operation and vulnerabilities than this report contains has already been --- and continues to be --- widely disseminated. For example, a paper written by staff of the Oak Ridge National Laboratory (ORNL) and the Defense Threat Reduction Agency (DTRA), published in 2004 in a technical journal and available on the Internet, contains a diagram of a generic nuclear power plant indicating where truck bombs of various sizes could be detonated in order to stage an attack with a 100% probability of core damage.

There can be little doubt that al Qaeda and other terrorist organizations are already well aware of the severity of the consequences that could result from an attack at Indian Point. It is NRC and FEMA that seem not to appreciate this risk, and it is to them above all that we direct this study. We also believe that there is a considerable cost, but no apparent benefit, to withholding information that could help people to protect themselves in the event of a terrorist attack at Indian Point. Better information will enable better coordination of all populations at risk and help to avoid situations where some individuals take inappropriate actions that endanger others.

This report would not have been necessary had we seen any indication that NRC and other government authorities fully appreciate the seriousness of the risk to the public from radiological sabotage, or if certain members of the Nuclear Regulatory Commission had not made statements regarding severe accident consequences and risks that contradicted the results of quantitative analyses developed and refined over several decades by NRC's own technical staff and contractors.

For instance, at a recent briefing on NRC's emergency preparedness program, NRC Commissioner Edward McGaffigan, comparing the radiological exposure from a reactor accident to air travel, radon and other sources of exposure to natural radioactivity, said that[12]

> "...the order of magnitude of the release is similar to all of these other things in people's lives and they should not panic over a few hundred millirem or even a couple of rem ... but it's this radiation phobia, absolutely inflamed by these anti-

[12] US NRC, *Briefing on Emergency Preparedness Program Status*, Public Meeting, September 24, 2003, transcript, p. 73.

> nuclear groups putting out their misinformation that actually hurts emergency planning ..."

Commissioner McGaffigan's statement is misleading on at least three counts:

(1) Current emergency planning guidance is already based on the principle that exposures of "a couple of rem" would be acceptable following a large radiological release;

(2) The potential doses from a large radiological release can greatly exceed "a few hundred millirem or even a couple of rem" far downwind of the release site, and for many individuals could result in a significant increase in their lifetime risk of cancer (10% or greater) or even pose a risk of severe injury or death from acute radiation exposure;

(3) Even if the average dose resulting from a large release were on the order of "a couple of rem," the total collective detriment (latent cancer fatalities and economic damages) could be very high if a large number of people in a densely populated area were so affected.

We believe that misinformation originating within NRC itself is the biggest obstacle to development of the robust radiological emergency planning strategies needed to cope with today's heightened threat. Statements like those cited above raise the concern that those responsible for regulating the nuclear industry and protecting it from terrorist attack are either in a chronic state of denial or actually believe the propaganda generated by the nuclear industry for public consumption. If this is indeed the case, then one cannot have confidence that emergency planning officials are basing their decisions on accurate and unbiased information. Since the departure of NRC Commissioner Greta Dicus a few years ago, the current Commission does not have any members with backgrounds in radiation protection and health issues. One wonders whether the NRC Commissioners truly understand and appreciate the full extent of the dangers posed by the facilities that they regulate.

(c) The CRAC2 Report

Given the lack of credible information from public officials on the potential consequences of a terrorist attack at Indian Point, concerned neighbors of the plant turned to one of the few sources on this subject in the public domain --- the so-called "CRAC2 Report," carried out by Sandia National Laboratories (SNL) under contract for NRC in 1981. This study, formally entitled "Technical Guidance for Siting Criteria Development," used a computer code developed by SNL known as CRAC2 ("Calculation of Reactor Accident Consequences") to analyze the consequences of severe nuclear plant accidents and to study their dependence on population density, meteorological conditions and other characteristics. The version of the CRAC2 Report that had been submitted to NRC for eventual public release only contained average values of consequence results,

but the "peak" values for worst-case weather conditions were obtained by Congressman Edward Markey in 1982 and provided to the Washington Post.[13]

At many reactor sites, the CRAC2 Report predicted that for unfavorable weather conditions, a severe nuclear reactor accident could cause tens of thousands of early fatalities as a result of severe radiation exposure, and comparable numbers of latent cancer fatalities from smaller exposures. For Indian Point 3 (which at the time operated at a significantly lower power than it now does), CRAC2 predicted peak values of 50,000 early fatalities and 14,000 latent cancer fatalities, with early fatalities occurring as far as 17.5 miles downwind of the site.

The CRAC2 Report only considered accidents affecting operating nuclear reactors, and did not evaluate the consequences of accidents also involving spent fuel storage pools. Spent fuel pool loss-of-coolant accidents could themselves result in large numbers of latent cancer fatalities, widespread radiological contamination and huge cleanup bills, even if only a fraction of the fuel in the pool were damaged.

The release of the CRAC2 figures caused a great deal of consternation, but NRC was able to defuse the controversy by claiming that the peak results corresponded to accidents with extremely low probabilities (said to be one in a billion), and hence were not a cause for concern. In fact, Robert Bernero, director of the NRC's risk analysis division at the time, said (in a moment of unfortunate prescience) that such severe accidents would be less likely than "a jumbo jet crashing into a football stadium during the Superbowl."[14]

When Riverkeeper and other groups dusted off and called attention to the CRAC2 Report following the September 11 attacks, the NRC appeared unable to appreciate the new relevance of the study in a world where the possibility of a jumbo jet crashing into the Superbowl was no longer so remote. For example, in rejecting a 2001 petition filed by Riverkeeper to shut down the Indian Point plant until Entergy implemented a number of prudent security-related measures, the NRC merely repeated its old probability-based arguments, saying that[15]

> "...the reactor siting studies in the CRAC2 Report ... used generic postulated releases of radioactivity from a spectrum of severe (core melt) accidents, independent of the probabilities of the event occurring or the impact of the mitigation mechanisms. The studies were never intended to be realistic assessments of accident consequences. The estimated deaths and injuries resulted from assuming the most adverse condition for each parameter in the analytical code. In the cited studies, the number of resulting deaths and injuries also reflected the assumption that no protective actions were taken for the first 24

[13] Subcommittee on Oversight & Investigations, Committee on Interior and Insular Affairs, U.S. House of Representatives, "Calculation of Reactor Accident Consequences (CRAC2) For U.S. Nuclear Power Plants Conditional on an 'SST1' Release," November 1, 1982.
[14] Robert J. McCloskey, "The Odds of the Worst Case," *Washington Post*, November 17, 1982.
[15] US Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Notice of Director's Decision Under 10 CFR 2.206, November 18, 2002.

> hours. The studies did not, and were never intended to, reflect reality or serve as a basis for emergency planning. The CRAC2 Report analyses used more simplistic models than current technologies."

Earlier in 2002, in a letter to the New York City Council, the NRC also said that[16]

> "The Sandia study does not factor in the numerous probabilistic risk studies that have been performed since 1982. More realistic, current inputs, assumptions, and modeling techniques would be expected to result in much smaller health consequences."

In a more recent "point paper" on homeland protection and preparedness, NRC continued to repeat these themes, although its conclusions were somewhat more equivocal: [17]

> "The Sandia Siting Study ["CRAC2"] ... was performed to develop technical guidance to support the formulation of new regulations for siting nuclear power reactors. A very large radiation release and delayed evacuation, among other factors, accounts for the more severe consequences ... As an overall conclusion, that report does not present an up-to-date picture of risk at nuclear plants and does not reflect current knowledge in probabilistic or phenomenological modeling.
>
> "Since September 11, 2001, the NRC has been performing assessments of the consequences of a terrorist attack on a nuclear power plant. These assessments are much more detailed than past analyses and reflect our improved understanding of severe accident phenomena. The more recent analyses have involved a more realistic assessment of the radiation release, emergency planning capabilities, radiation spreading, and health effects. More recent analysis indicates a general finding that public health effects from terrorist attacks at most sites are likely to be relatively small."

Although NRC continues to harshly criticize the CRAC2 Report and anyone who cites its results, it has not publicly identified the "more realistic, current inputs, assumptions and modeling techniques that would be expected to result in much smaller health consequences," much less demonstrated the validity of these results by providing the public with its calculations for independent review. In fact, NRC now considers that these analyses are too sensitive for public release, making it impossible for the public to verify its claims.

NRC's unwillingness to share this kind of information with the public is not unexpected. NRC (like its predecessor, the Atomic Energy Commission) has worked over its history to shield the public from estimates of the consequences of severe accidents without simultaneous consideration of the low probabilities of such accidents. By multiplying

---

[16] Hubert Miller, Region I Administrator, US NRC, letter to Donna De Constanzo, Legislative Attorney, New York City Council, July 24, 2002.

[17] US Nuclear Regulatory Commission, "Point Paper on Current Homeland Protection and Preparedness Issues," November 2003, on the NRC Web site, www.nrc.gov.

high consequence values with very low probability numbers, the consequence figures appear less startling to the layman but are obscured in meaning. For instance, a release that could cause 100,000 cancer fatalities would only appear to cause 1 cancer fatality per year if the associated probability of the release were 1/100,000 per year.

This issue was central to the so-called Indian Point Special Proceeding, a 1983 review conducted by a panel of NRC administrative judges that examined whether Indian Point posed unusually high risks because of its location in the densely populated New York metropolitan area. Before this proceeding, the NRC ruled that all testimony on accident consequences must also contain a discussion of accident probabilities. However, in its decision, the three-judge Atomic Safety and Licensing Board panel concluded that "the Commission should not ignore the potential consequences of severe-consequence accidents by always multiplying those consequences by low probability values."[18] One of the judges dissented from this majority opinion, insisting that singling out Indian Point "to the exclusion of many other sites similarly situated in effect raises again the question of considering consequences without their associated probabilities. This we have been restricted from doing by the Commission."[19] Today, it appears that this minority opinion ultimately prevailed at NRC.

The results of the CRAC2 Report are indeed of questionable applicability today. But the reasons for this are not the ones that NRC has identified, but include, for example, the fact that the CRAC2 Report

- used census data from 1970, at a time before rampant suburban sprawl greatly increased the population densities in formerly rural areas close to some nuclear reactor sites;

- assumed that the entire 10-mile emergency planning zone would be completely evacuated within at most six hours after issuance of a warning (contrary to NRC's assertion that the CRAC2 peak results reflect the assumption that "no protective actions were taken for the first 24 hours"), whereas the current evacuation time estimate for the Indian Point EPZ, based on updated assessments of likely road congestion, is nearly ten hours;

- assumed aggressive medical treatment for all victims of acute radiation exposure in developing estimates of the number of early fatalities, and employed a now-obsolete correlation between radiation dose and cancer risk that underestimated the risk by a factor of 4 relative to current models;

- sampled only 100 weather sequences out of 8760 (an entire year's worth), a method which we find underestimates the peak value occurring over the course of a year by 30%.

---

[18] US Nuclear Regulatory Commission, Atomic Safety and Licensing Board, Indian Point Special Proceeding, Recommendations to the Commission, October 24, 1983, p. 107.
[19] Ibid, "Dissenting Views of Judge Gleason," p. 433.

In 1990, the CRAC2 code was retired in favor of a new code known as MACCS ("MELCOR Accident Consequence Code System"), which was updated to MACCS2 in 1997. The MACCS2 code, also developed by Sandia National Laboratories, is the state-of-the-art consequence code employed by both NRC and DOE in conducting dose assessments of radiological releases to the atmosphere. It includes numerous improvements over the CRAC2 code.[20]

However, the fundamental physics models that form the basis for both the CRAC2 and MACCS2 codes have not changed in the past two decades. Nor has evidence arisen since the CRAC2 Report was issued that would suggest that the CRAC2 "source term" --- that is, the fraction of the radioactive contents of the reactor core assumed to be released to the environment during a severe accident --- significantly overestimated potential releases. On the contrary, the Chernobyl disaster in 1986 demonstrated that such large releases were possible.[21] The state-of-the art revised source term developed by NRC, as defined in the NRC report NUREG-1465, "Accident Source Terms for Light-Water Nuclear Power Plants," is little different from the source terms used in the CRAC2 Report.[22] Recent experimental work, including the Phébus tests in France, have provided further confirmation of the NUREG-1465 source term.[23] Other tests, such as the VERCORS experiments in France, have found that NUREG-1465 actually underestimates the releases of some significant radionuclides.

The NRC continues to stress the absence of consideration of accident probabilities in dismissing the results of the CRAC2 Report. However, this criticism is invalid in the post-9/11 era. Accident probabilities are not relevant for scenarios that are intentionally caused by sabotage. Severe releases resulting from the simultaneous failure of multiple safety systems, while very unlikely if left up to chance, are precisely the outcomes sought by terrorists seeking to maximize the impact of their attack. Thus the most unlikely accident sequences may well be the most likely sabotage sequences.

---

[20] D.I. Chanin and M.L. Young, *Code Manual for MACCS2: Volume 1, User's Guide*, SAND97-0594, Sandia National Laboratories, March 1997.

[21] The nuclear industry often argues that a Chernobyl-type accident could not happen in the United States because the reactor was of a different and inferior type to US plants and lacked a robust containment structure. While it is true that the specific accident sequence that led to the destruction of the Chernobyl-4 reactor and the resulting radiological release was characteristic of graphite-moderated reactors like Chernobyl and would not likely occur at a US light-water reactor (LWR), it is simply false to claim that there are no possible accident sequences that could result in consequences similar to those of Chernobyl --- namely, core melt, loss or bypass of containment, and large radiological release to the environment. In fact, because such an event is not as likely to be as energetic as the Chernobyl explosion, and the plume is not likely to be as hot as the Chernobyl plume (which was fed by the burning of a large mass of graphite), the radiological release from a severe accident at a US LWR will not rise as high or disperse as far. Therefore, radiological exposure to the public near a US LWR could be far greater than was the case at Chernobyl, because the plume would be more concentrated closer to the plant.

[22] L. Soffer, et al., *Accident Source Terms for Light-Water Nuclear Power Plants, Final Report,* NUREG-1465, US NRC, February 1995.

[23] US NRC, Memorandum from Ashok Thadani to Samuel J. Collins, "Use of Results from Phébus-FP Tests to Validate Severe Accident Codes and the NRC's Revised Accident Source Term (NUREG-1465)," Research Information Letter RIL-0004, August 21, 2000.

Other aspects that add an element of randomness to accident scenarios, such as meteorological conditions, can also be controlled through the advance planning and timing of a terrorist attack. Therefore, even if NRC were correct in claiming that the CRAC2 Report assumes the "most adverse condition" for each accident-related parameter, such an approach would still be appropriate for analyzing the potential maximum consequences of a sophisticated terrorist attack.

We have not been able to identify any issues that would suggest the consequence estimates provided in the CRAC2 Report were significantly overstated. But in light of the problems with the CRAC2 Report discussed earlier, we have conducted our own analysis of the consequences of a sophisticated terrorist attack at the Indian Point plant, using the MACCS2 code and the most up-to-date information available. This included the NUREG-1465 revised source term, the most current dose conversion and cancer risk coefficients recommended by the International Commission on Radiological Protection (ICRP), and the most recent evacuation time estimate (ETE) for Indian Point developed by consultants for Entergy Nuclear, the plant operator. We used the SECPOP2000 code, developed for NRC by Sandia National Laboratories, to generate a high-resolution MACCS2 site data file that includes a regional population distribution based on 2000 Census data and an economic data distribution based on 1997 government statistics.

For Indian Point, we find that the MACCS2 results for peak early fatalities are generally consistent with the CRAC2 Report, but that the CRAC2 Report significantly underestimates the peak number of latent cancer fatalities that could occur.

Moreover, the consequence estimates in this report are based on a number of optimistic assumptions, or "conservatisms," that tend to underestimate the true consequences of a terrorist attack at Indian Point. For example:

1. We use an evacuation time estimate that assumes the attack takes place in the summer in good weather, and does not take into account the possibility that terrorists may time their attack when evacuation is more difficult or actively interfere with the evacuation.

2. We only consider the permanent resident population of the 10-mile plume exposure EPZ, and not the daily transient population, which would increase the total population of the EPZ by about 25%.

3. We use values for the rated power of the Indian Point reactors from 2002 that are about 5% lower than the current values.

4. The only health consequences we consider are early fatalities from acute radiation syndrome and latent fatalities from cancer. We do not assess the excess mortality associated with the occurrence of other well-documented health effects of radiation such as cardiovascular disease. We also do not consider non-fatal effects of radiation, such as the reduction in intelligence quotient (IQ) of children irradiated in utero or other birth defects.

5. The NUREG-1465 source term does not represent the maximum possible radiological release from a core melt. Also, the assumed delay time between the attack and the start of the radiological release is nearly two hours, which is not nearly as short as the minimum of 30 minutes that is contemplated in NRC's emergency planning regulations.

6. The calculations assume only that the reactors itself are attacked and that the large quantity of spent fuel in the wet storage pools remains undamaged.

In the following sections, we discuss some technical issues related to severe accident and sabotage phenomena. Then we describe the methodology, tools and input parameters used to carry out the calculation. Finally, we present our results and conclusions.

ACCIDENTS: DESIGN-BASIS, BEYOND-DESIGN-BASIS, AND DELIBERATE

The NRC has traditionally grouped nuclear reactor accidents into two main categories: "design-basis" accidents, and "beyond-design-basis" or "severe" accidents.

(a) Design-basis accidents

Design-basis accidents are accidents that nuclear plants must be able to withstand without experiencing unacceptable damage or resulting in radiological releases that exceed the regulatory limits known as "Part 100" releases (because of where they can be found in the NRC regulations).

One of the more challenging design-basis accidents for pressurized-water reactors (PWRs) like those at Indian Point is a loss-of-coolant accident (LOCA). In the "primary" system of a PWR, the reactor core, which is contained in a steel vessel, is directly cooled by the flow of high-pressure water forced through pipes. In a LOCA, a pipe break or other breach of the primary system results in a loss of the water essential for removing heat from the reactor fuel elements. Even if the nuclear reactor is immediately shut down or "scrammed," an enormous quantity of heat is still present in the fuel, and cooling water must be restored before a significant number of fuel elements reach temperatures above a critical limit. If heated beyond this limit, the fuel element cladding can become brittle and shatter upon contact with cooling water. Eventually, the core geometry can become "uncoolable" and the fuel pellets themselves will reach temperatures at which they start to melt.

In a design-basis LOCA, it is assumed that the emergency core cooling system (ECCS) works as designed to provide makeup coolant water to the nuclear fuel, terminating the event before it becomes impossible to control. Even in this case, however, a significant fraction of the radioactive inventory in the core could be released into the coolant and transported out of the primary system through the pipe break. The primary system therefore must be enclosed in a leak-tight containment building to ensure that Part 100 limits are not exceeded in the event of a design-basis LOCA. To demonstrate compliance with Part 100, dose calculations at the site boundary are carried out by specifying a so-called "source term" --- the radioactive contents of the gases within the containment following the LOCA --- and assuming that the containment building leaks at its maximum design leak rate, typically about 0.1% per day. Such an event was historically considered a "maximum credible accident."

(b) Beyond-design-basis accidents

In contrast to design-basis accidents, "beyond-design-basis" accidents (also known as "severe" accidents) are those in which multiple failures occur, backup safety systems do not work as designed, the core experiences a total "meltdown" and radiological releases far greater than the Part 100 limits become possible. For example, if the ECCS does not work properly after a LOCA, the core will continue to overheat, eventually forming a

molten mass that will breach the bottom of the steel reactor vessel and drop onto the containment floor. It will then react violently with any water that is present and with concrete and other materials in the containment. At this point, there is little hope that the event can be terminated before much of the radioactive material within the fuel is released in the form of gases and aerosols into the containment building.

Even worse is the potential for mechanisms such as steam or hydrogen explosions to rupture the containment building, releasing its radioactive contents into the environment. Although not the only distinguishing feature, a major distinction between design-basis and severe accidents is whether containment integrity is maintained. Even a small rupture in the containment building --- no more than a foot in diameter --- would be sufficient to depressurize it and to vent the gases and aerosols it contains into the environment in less than half an hour.[24] This would result in a catastrophic release of radioactivity on the scale of Chernobyl, and Part 100 radiation exposure limits would be greatly exceeded.

The containment building can also be "bypassed" if there is a rupture in one of the interfaces between the primary coolant system and other systems that are outside of containment, such as the "secondary" coolant system (the fluid that drives the turbine generators) or the low-pressure safety injection system. For instance, the rupture in the steam generator that occurred at Indian Point 2 in February 2000 created a pathway in which radioactive steam from the primary system was able to pass into the secondary system, which is not enclosed in a leak-tight boundary. If that event had coincided with significant fuel damage, the radiological release to the environment could have been far greater.

NRC has always had an uncomfortable relationship with beyond-design-basis accidents. By their very definition, they are accidents that were not considered in the original design basis for the plant. In fact, according to NRC, "the technical basis for containment design was intended to ensure very low leakage under postulated loss-of-coolant accidents. No explicit consideration was given to performance under severe accidents."[25] Indeed, NRC has never instituted a formal regulatory requirement that severe accidents be prevented. In 1985, the Commission ruled by fiat in its Severe Accident Policy Statement that "existing plants pose no undue risk to health and safety" and that no regulatory changes were required to reduce severe accident risk. NRC's basic assumption is that if a plant meets design basis requirements, then it will have sufficient resistance against severe accidents, and it has devoted considerable resources to the task of "confirmatory research" to justify this assumption. NRC believes that this approach provides "adequate protection" of public health and safety because the probability of a

---

[24] US Nuclear Regulatory Commission, *Preliminary Assessment of Core Melt Accidents at the Zion and Indian Point Nuclear Power Plants and Strategies for Mitigating Their Effects, Analysis of Containment Building Failure Modes, Preliminary Report*, NUREG-0850, Vol. 1, November 1981, p. 3-2.
[25] US Nuclear Regulatory Commission, *Reactor Risk Reference Document (Appendices J-0)*, NUREG-1150, Draft for Comment, February 1987, p. J.10-1.

severe accident capable of rupturing or bypassing the containment prior to effective evacuation of the EPZ is so low in most cases as to be below regulatory concern.[26]

(c) "Deliberate accidents"

It is true that a spontaneous occurrence of the multiple system failures necessary to cause a severe accident and large radiological release is typically a very improbable event. However, if one considers the possibility of sabotage or "deliberate" accidents, the low-probability argument that NRC uses to justify the continued operation of nuclear plants completely breaks down. Terrorists with basic and readily available knowledge of how nuclear plants operate can design their attack to maximize the chance of achieving a core melt and large radiological release. With modest inside assistance, as contemplated by NRC in its regulations and practices, saboteurs would be able to identify a plant-specific set of components known as a "target set." If all elements of a target set are disabled or destroyed, significant core damage would result. Thus, by deliberately disrupting all redundant safety systems, saboteurs can cause a severe event that would have had only a very low probability of occurrence if left to chance.

The likelihood of a successful attack is enhanced for plants with "common-cause" failure modes. A common-cause failure is a single event that can lead to the failure of multiple redundant systems. For example, if the diesel fuel supplied to a nuclear plant with two independent emergency diesel generators from the same distributor is impure, then both generators may fail to start for the same reason if off-site power is lost and emergency power is needed. This would result in a station blackout, one of the most serious challenges to pressurized-water reactors like Indian Point. While some common-cause failure modes can be corrected, others are intrinsic to the design of currently operating nuclear plants. Common-cause failure modes make the saboteurs' job easier, as fewer targets would have to be disabled to achieve the desired goal.

In addition to causing a core meltdown, terrorists also have the means to ensure that the radioactive materials released from the melting fuel can escape into the environment by breaching, severely weakening or bypassing the containment.[27] Finally, saboteurs can maximize the harm caused by a radiological release by staging their attack when the meteorological conditions favor a significant dispersal over densely populated areas, and even interfering with the execution of emergency plans.

NRC has formally maintained for at least two decades that it does not make sense to assign probabilities to terrorist attacks. In a 2002 memorandum, NRC stated that[28]

> "the horrors of September 11 notwithstanding, it remains true that the likelihood of a terrorist attack being directed at a particular nuclear facility is not

[26] There have been situations where NRC concluded that "adequate protection" was not met at certain nuclear plants and required additional safety measures. However, such instances are rare.
[27] We have decided not to describe such means in greater detail, although we have little doubt that terrorists are already familiar with them.
[28] US NRC, Memorandum and Order, CLI-02-025, December 18, 2002, p. 17.

> quantifiable. Any attempt at quantification or even qualitative assessment would be highly speculative. In fact, the likelihood of attack cannot be ascertained with confidence by any state-of-the-art methodology ... we have no way to calculate the probability portion of the [risk] equation, except in such general terms as to be nearly meaningless."

Yet at other times, NRC does not hesitate to invoke probabilities when arguing that the public has nothing to fear from terrorist attacks on nuclear plants. For example, here is what NRC has to say about the CRAC2 study in its recent "point paper" on homeland protection and preparedness:[29]

> "Over the years, the NRC has performed a number of consequence evaluations to address regulatory issues ... We have considered the extent to which past analyses, often the subject of public statements by advocacy groups and the media, can be superceded [sic] by more recent analysis ... Past studies usually have considered ... a number of scenarios, which resulted in only minor consequences. The most limiting severe scenarios, which comprise a minority of the calculations and represent *very low probability events* [emphasis added], are the predictions typically cited in press accounts. These scenarios have assumed ... very large radiation releases, bounding emergency response assumptions or bounding conditions (including weather) for the spread of the radiation. The combination of these factors produces large and highly unlikely results."

These two excerpts are inconsistent. If it is meaningless to quantify the likelihood of a terrorist attack, then one cannot dismiss the possibility of terrorist attacks causing the most severe consequences by claiming they are "highly unlikely." Therefore, in order to base emergency planning on the best possible information, NRC must accept the fact that the growing threat of domestic terrorism has forever altered the delicate risk calculus that underlies its approach to safety regulation. NRC can no longer shy away from confronting the worst-case consequences of terrorist attacks on nuclear power plants. And perhaps the most attractive target in the country, where the consequences are likely to be the greatest, is Indian Point.

[29] US NRC, "Point Paper on Current Homeland Protection and Preparedness Issues" (2003), op cit.

THE HEALTH CONSEQUENCES OF A RADIOLOGICAL RELEASE FROM INDIAN POINT

The Indian Point power plant is located on 239 acres on the Hudson River in the village of Buchanan in Westchester County, New York. There are two operating pressurized-water reactors (PWRs) on site, Indian Point 2, rated at 971 MWe, and Indian Point 3, rated at 984 MWe. Both reactors are operated by Entergy Nuclear.

Indian Point is located in one of the most densely populated metropolitan areas in the United States, situated about 24 miles from the New York City limits and 35 miles from midtown Manhattan. Extrapolating from 2000 Census data, in 2003 over 305,000 persons resided within the roughly ten-mile radius plume exposure emergency planning zone for Indian Point, and over 17 million lived within 50 miles of the site.[30]

The types of injury that may occur following a catastrophic release of radioactive material resulting from a terrorist attack at Indian Point fall into two broad categories. The first category, "early" injuries and fatalities, are those that are caused by short-term whole-body exposures to doses of radiation high enough to cause cell death. Early injuries include the constellation of symptoms known as **acute radiation syndrome** that should be familiar to anyone who has read *Hiroshima* by John Hersey --- gastrointestinal disturbance, epilation (hair loss) and bone marrow damage. Other early injuries include severe skin damage, cataracts and sterility. For sufficiently high doses, early fatalities --- death within days or weeks --- can occur. These so-called "deterministic" effects are induced only when levels of radiation exposure exceed certain thresholds.

Another class of injury caused by ionizing radiation exposure is genetic damage that is insufficient to cause cell death. At doses below the thresholds for deterministic effects, radiation may cause damage to DNA that interferes with the normal process of cell reproduction. This damage can eventually lead to cancer, which may not appear for years or even decades, depending on the type. Because a single radiation-induced DNA lesion is believed to be capable of progressing to cancer, there is no threshold for these so-called "stochastic" effects.[31]

The clinical response of individuals to ionizing radiation exposure is highly variable from person to person. Some individuals have a lower capability of DNA repair and thus are more susceptible to the carcinogenic effects of radiation --- a condition that is most severe in people with certain genetic diseases like ataxia telangiectasia. Children are particularly vulnerable to radiation exposure. For the same degree of exposure to a

---

[30] A figure of 20 million people within 50 miles of Indian Point has often been quoted. This value may have been obtained by summing the populations of all counties that are either totally or partially within the 50-mile zone.

[31] A small but vocal group of pro-nuclear activists continue to maintain, in the face of overwhelming scientific evidence to the contrary, that a threshold dose exists below which ionizing radiation may have no effect or even may provide health benefits. However, there is a growing body of experimental data that indicates that low-dose radiation may actually be a more potent carcinogen than high-dose radiation because of low-dose "bystander effects."

radioactive plume, children will receive a greater absorbed dose than adults because of their lower body weight and higher respiration rate, even though their lung capacity is smaller. And because children and fetuses have much higher growth rates than adults, the same radiation dose has a greater chance of causing cancer in children and fetuses than in adults.

Exposure to low-dose ionizing radiation has also been associated with excess mortality from diseases other than cancer, such as cardiovascular disease, possibly as a result of radiation-induced inflammation. There is growing evidence that the effect of low-dose radiation exposure on mortality from diseases other than cancer may be as great as its effect on mortality from cancer, implying that current, cancer-based risk estimates may be too low by a factor of two.[32]

A radiological release from a nuclear plant accident would consist of many different types of radioactive materials. Some isotopes, such as cesium-137, emit penetrating gamma rays and can cause radiation injury from outside of the body. Other isotopes do not emit radiation that can penetrate skin but are most dangerous when inhaled or ingested, where they can concentrate in internal organs and deliver high doses to surrounding tissue. Iodine-131, which concentrates in the thyroid gland, and strontium-90, which concentrates in teeth and bones, are in this category. Some isotopes have short half-lives and do not persist in the environment, while others are long-lived and can result in long-term contamination.

NRC requires that evacuation planning in the event of a radiological emergency take place only within the so-called "plume exposure" emergency planning zone (EPZ), a roughly circular area with a radius of approximately ten miles. The choice of this distance was based in part on NRC analyses indicating that in the event of a severe accident, dose rates high enough to cause early fatalities from acute radiation syndrome would be confined to a region within about ten miles of the release point. However, dose rates outside of this region, although on average not high enough to cause early fatalities, could be high enough to result in a significant risk of cancer unless effective protective measures are taken. NRC's emergency planning regulations were never designed to limit such exposures in the event of the "worst core melt sequences," for which the protection goal is that "immediate life threatening doses would generally not occur outside the zone."[33]

Thus the current emergency planning basis is not now, and never was, intended to protect the public from significant but not immediately lethal exposures in the event of the "worst core melt sequences," such as those that could result from a well-planned terrorist attack. It should therefore be no surprise that NRC's emergency planning procedures

---

[32] A. MacLachlan, "UNSCEAR Probes Low-Dose Radiation Link to Non-Cancer Death Rate," *Nucleonics Week*, June 17, 2004.
[33] US NRC, *Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Plants*, NUREG-0654, 1980, p. 12.

would not protect individuals either inside or outside the EPZ from such exposures in the event of an attack.

The proximity of Indian Point to New York City, its populous suburbs and its watershed, given the potential hazard it represents, has long been an issue of concern and controversy. Following the Three Mile Island accident in March 1979, the Union of Concerned Scientists (UCS) unsuccessfully petitioned the NRC to suspend operations at Indian Point, in part because of its location in a densely populated area. At the same time, the NRC formed two task forces to examine the risks posed by Indian Point and the Zion plant near Chicago "because of the high population densities surrounding those units" and initiated a formal adjudication, the Indian Point Special Proceeding, to review the issues raised in the UCS petition and others.[34]

During the Special Proceeding, three NRC administrative judges heard testimony regarding the potential impacts of a severe accident at Indian Point on New York City residents. For instance, the director of New York City's Bureau of Radiation Control testified that potassium iodide (KI), which can block the uptake of radioactive iodine by the thyroid if taken near the time of exposure, should be stockpiled for "possible immediate use in New York City," at a time when NRC did not recommend that KI be provided even for residents of the 10-mile EPZ.

The administrative judges reached some disturbing conclusions in the proceeding. They stated that "under certain meteorological conditions, delayed fatalities from cancer appear to be possible almost anywhere in the city" and that "a severe release at Indian Point could have more serious consequences than that same release at virtually any other site licensed by the Commission." And they urged the Commission "to give serious consideration to the potential costs to society of dangerous, low probability accidents. Such accidents could, as Staff testimony has shown, result in fatalities that number in the hundreds or thousands."

The Commission appears to have essentially forgotten these conclusions. Many of the technical issues resolved during the course of the Special Proceeding are being debated all over again today.

[34] US NRC, Indian Point Special Proceeding, 1983, p. 5.

THE MACCS2 CODE

MACCS2 is a computer code that was developed by Sandia National Laboratories under NRC sponsorship as a successor to CRAC2.[35] It is designed to estimate the health, environmental and economic consequences of radiation dispersal accidents, and is widely used by NRC and DOE for various safety applications. It utilizes a standard straight-line Gaussian plume model to estimate the atmospheric dispersion of a point release of radionuclides, consisting of up to four distinct plumes, and well-established models to predict the deposition of radioactive particles on the ground from both gravitational settling ("dry deposition") and precipitation ("wet deposition").[36] From the dispersion and deposition patterns, the code can then estimate the radiation doses to individuals as a result of external and inhalation exposures to the radioactive plume and to external radiation from radionuclides deposited on the ground ("groundshine"). The code also has the capability to model long-term exposures resulting from groundshine, food contamination, water contamination and inhalation of resuspended radioactive dust.

The code also can evaluate the impact of various protective actions on the health and environmental consequences of the release, including evacuation, sheltering and, in the long term, remediation or condemnation of contaminated areas. Most parameters, such as the average evacuation speed, decontamination costs, and the dose criteria for temporary relocation and long-term habitation, can be specified by the user.

MACCS2 requires a large number of user-specified input parameters. A given release is characterized by a "source term," which is defined by its radionuclide content, duration and heat content, among other factors. The shape of the Gaussian plume is determined by the wind speed, the release duration, the atmospheric stability (Pasquill) class and the height of the mixing layer at the time of the release.

MACCS2 requires the user to supply population and meteorological data, which can range from a uniform population density to a site-specific population distribution on a high-resolution polar grid. The meteorological data can range from constant weather conditions to a 120-hour weather sequence. The code can process up to 8760 weather sequences --- a year's worth --- and generate a frequency distribution of the results.

The code allows the user to define the dose-response models for early fatalities (EFs) and latent cancer fatalities (LCFs). We use the MACCS2 default models. For EFs, MACCS2 uses a 2-parameter hazard function, with a default LD_{50} dose (the dose associated with a 50% chance of death) of 380 rem. LCFs, MACCS2 uses the standard linear, no-threshold model, with a dose-response coefficient of 0.1 LCF/person-Sievert and a dose-dependent reduction factor of 2, per the 1991 recommendations of the International Committee on

[35] Chanin and Young (1997), op cit.

[36] Much of the following section is based on a recent comprehensive review of MACCS2 by the Department of Energy, which we would recommend to readers interested in a more in-depth discussion of the capabilities and limitations of the code. See Office of Environment, Safety and Health, U.S. Department of Energy, *MACCS2 Computer Code Application Guidance for Documented Safety Analysis: Interim Report*, DOE-EH-4.2.1.4-Interim-MACCS2, September 2003.

Radiological Protection (ICRP) in ICRP 60.[37] The corresponding coefficients used in the CRAC2 model, based on now-antiquated estimates, were lower by a factor of 4.

For the calculation of the committed effective dose equivalent (CEDE) resulting from inhalation and ingestion of radionuclides, we have replaced the default MACCS2 input file with one based on the more recent dose conversion factors in ICRP 72.[38] We have shown previously that this substitution reduces the projected number of latent cancer fatalities from a severe nuclear reactor accident by about one-third.[39] (The default MACCS2 file incorporates EPA guidance based on ICRP 30, which although out of date continues to be the basis for regulatory analyses in the United States.)

When using MACCS2 several years ago, we discovered an error that resulted in an overcounting of latent cancer fatalities in the case of very large releases. After pointing this out to the code manager, SNL sent us a revised version of the code with the error corrected, which we have used for the analysis in this report.

Like most radiological consequence codes in common use, MACCS2 has a number of limitations. First of all, because it incorporates a Gaussian plume model, the speed and direction of the plume are determined by the initial wind speed and direction at the time of release, and cannot change in response to changing atmospheric conditions (either in time or in space). Consequently, the code becomes less reliable when predicting dispersion patterns over long distances and long time periods, given the increasing likelihood of wind shifts. Also, the Gaussian plume model does not take into account terrain effects, which can have a highly complex impact on wind field patterns and plume dispersion. And finally, MACCS2 cannot be used for estimating dispersion less than 100 meters from the source.

However, MACCS2 is adequate for the purpose of this report, which is to develop order-of-magnitude estimates of the radiological consequences of a catastrophic attack at Indian Point for residents of New York City and the entire New York metropolitan area, and to assess the impact of different protective actions on these consequences. We restrict our evaluations to a circular area with a radius of 50 miles centered on Indian Point, except for the calculation of long-term doses and economic impacts, which we assess out to 100 miles.

In the next section, we discuss the basis for the MACCS2 input parameters that we use in our evaluation.

---

[37] MACCS2 does not allow the user to specify different dose-response models for different radionuclides. We use a model with a dose-dependent reduction factor of 2, even though this assumption likely underestimates the carcinogenic potential of alpha-emitters, which is not reduced in effectiveness at low doses or dose rates.

[38] International Commission on Radiological Protection (ICRP), *Age-Dependent Doses to Members of the Public from Intake of Radionuclides: Part 5, Compilation of Ingestion and Inhalation Dose Coefficients*, ICRP Publication 72, Pergamon Press, Oxford, 1996.

[39] E. Lyman, "Public Health Risks of Substituting Mixed-Oxide for Uranium Fuel in Pressurized-Water Reactors," *Science and Global Security* **9** (2001), pgs. 33-79. See Footnote 48.

THE SABOTAGE SCENARIO

The scenario that we analyze is based on the so-called "revised source term" that NRC defined in 1995 in NUREG-1465. The revised source term was developed as a more realistic characterization of the magnitude and timing of radionuclide releases during a core-melt accident than the source term originally specified for use in Part 100 siting analyses. In its entirety, the PWR revised source term presented in NUREG-1465 corresponds to a severe accident in which the primary coolant system is depressurized early in the accident sequence. An example is a "large break loss-of-coolant accident" (LBLOCA), in which primary coolant is rapidly lost and the low-pressure safety injection system fails to operate properly, resulting in core melt and vessel failure. This scenario is one of the most severe events that can occur at PWRs like Indian Point, and could result in a relatively rapid release of radioactivity.

(a) The source term

A severe accident of this type would progress through four distinct phases. As the water level in the core decreases and the fuel becomes uncovered, the zirconium cladding tubes encasing the fuel rods overheat, swell, oxidize and rupture. When that occurs, radionuclides that have accumulated in the "gap" between the fuel and the cladding will be released into the reactor coolant system. If there is a break in the reactor coolant system (as would be the case in a LBLOCA), then these radionuclides would be released into the atmosphere of the containment building. These so-called "gap" releases consist of the more volatile radionuclides contained in irradiated fuel, such as isotopes of krypton, xenon, iodine and cesium. This period is known as the "gap release" phase, and is predicted to last about 30 minutes. The oxidation of the zirconium cladding by water also generates hydrogen, which is a flammable gas.

As the core continues to heat up, the ceramic fuel pellets themselves begin to melt, releasing greater quantities of radionuclides into the reactor vessel and through the breach in the reactor coolant system into the containment building atmosphere. The molten fuel mass then collapses and drops to the bottom of the reactor vessel, where it aggressively attacks the steel, melts through the bottom and spills onto the floor of the containment building.[40] The period between the start of fuel melting and breach of the reactor vessel is known as the "early in-vessel" phase, and typically would last about an hour.

When the molten fuel breaches the reactor vessel and drops to the containment building floor, it violently reacts with any water that has accumulated in the cavity and with the concrete floor itself. This "core-concrete interaction" causes further releases of radionuclides from the molten fuel into the containment building. This period is known as the "ex-vessel" phase, and would last for several hours.

[40] This scenario is not theoretical. During the 1979 accident at Three Mile Island Unit 2, part of the melted core relocated to the bottom of the reactor vessel where it began melting through the steel. The re-introduction of forced cooling water flow terminated this sequence before vessel failure.

At the same time, some portion of the molten core may remain in the reactor vessel, where it would continue to degrade in the presence of air and release radionuclides. Also, radionuclides released during the in-vessel phase that deposit on structures within the primary coolant system may be re-released into the containment building. These releases take place during the "late in-vessel" phase and could continue for many hours.

At the time when the molten core falls to the floor of the reactor vessel, steam explosions may occur that could blow apart the reactor vessel, creating high-velocity "missiles" that could rupture the containment building and violently expel the radioactive gases and aerosols it contains into the environment. This would result in a shorter in-vessel phase. If the vessel remains intact until melt-through, hydrogen or steam explosions are also possible when the molten fuel spills onto the concrete below the vessel, providing another opportunity for containment failure.

The complete revised source term (all four phases) is a general characterization of a low-pressure severe accident sequence, such as a large-break loss of coolant accident with failure of emergency core cooling systems. According to the timing of the accident phases in the revised source term, the "gap release" phase would begin within a few minutes after the initiation of the event and lasts for 30 minutes. At that time, the early in-vessel phase begins as the fuel pellets start to melt. This phase is assumed to last for 1.3 hours, and ends when the vessel is breached.

In our scenario, we assume that the attackers have weakened but not fully breached the containment, so that there is a high probability that the containment building will be ruptured by a steam or hydrogen explosion at the time of vessel breach. This results in a rapid purge of the radionuclide content of the containment building atmosphere into the environment, followed by a longer-duration release due to core-concrete interactions and late in-vessel releases.

We do not wish to discuss in detail how saboteurs could initiate this type of accident sequence. However, since NRC asserts that even in a terrorist attack these events are unlikely to occur, we need to present some evidence of the plausibility of these scenarios. One such scenario would involve a 9/11-type jet aircraft attack on the containment building, possibly accompanied by a ground attack on the on-site emergency power supplies. (One must also assume that interruption of off-site power takes place during an attack, given that off-site power lines are not under the control of the licensee and are not protected.)

The Nuclear Energy Institute (NEI) issued a press release in 2002 describing some of the conclusions of a study conducted by the Electric Power Research Institute (EPRI) that purported to show that penetration of a PWR containment by a jet aircraft attack was impossible. A study participant later acknowledged that (1) the justification for limiting the impact speed to 350 mph was based on pilot interviews and not on the results of simulator testing, and (2) even at 350 mph, their analysis actually found that the 42-inch

thick reinforced concrete containment dome of a PWR suffered "substantial damage" and the steel liner was deformed.[41]

However, even if penetration of the containment does not occur, the vibrations induced by the impact could well disrupt the supports of the coolant pumps or the steam generators, causing a LBLOCA. The emergency core cooling system pumps, which require electrical power, would not be available under blackout conditions caused by the disabling of both off-site and on-site power supplies. Thus makeup coolant would not be provided, the core would rapidly become uncovered and the NUREG-1465 sequence would begin. Other engineered safety features such as containment sprays and recirculation cooling would not be available in the absence of electrical power. The damaged containment building would then be far less resistant to the pressure pulse caused by a steam spike or hydrogen explosion, and would have a much higher probability of rupture at vessel breach. We note that the steel liner of a reinforced concrete containment structure like that at Indian Point only carries 10 to 20% of the internal pressure load, and therefore may fail well before the design containment failure pressure is reached if the concrete shell is damaged.

Because the emergency diesel generators are themselves quite sensitive to vibration, a ground assault may not even be necessary to disable them, since the aircraft impact itself, followed by a fuel-air explosion, could cause them to fail.

One can find support for the credibility of this scenario in the recently leaked summary of a report prepared for the German Environment Ministry by the nuclear safety consultant GRS on the vulnerability of German nuclear reactors to aircraft attacks.[42] In the summary, GRS defined a series of credible damage scenarios and then determined whether or not the resulting accident sequence would be controllable The report considered an attack on the Biblis B PWR by a small jet (Airbus A320) or medium-sized jet (Airbus A300) travelling at speeds from 225 to 394 miles per hour, where the peak speed of 394 mph was determined through the use of simulators. GRS concluded that for an event in which the jet did not penetrate the containment, but the resulting vibrations caused a primary coolant leak, and the control room was destroyed by debris and fire (a condition similar to a station blackout), then control of the sequence of events would be "uncertain."[43] Biblis B was designed for protection against the crash of a 1960s-era Starfighter jet and as a result is equipped, like most German reactors, with a double containment. In contrast, Indian Point 2 and 3, while of the same 1970s vintage as Biblis B, were not designed to be resistant to airplane crashes, and do not have double containments.

---

[41] R. Nickell, "Nuclear Plant Structures: Resistance to Aircraft Impact," 44th Annual Meeting of the Institute of Nuclear Materials Management, Phoenix, AZ, July 13-17, 2003.
[42] Mark Hibbs, "Utilities Expect Showdown with Trittin over Air Terror Threat," *Nucleonics Week* **45**, February 12, 2004.
[43] Gesellschaft für Anlagen und Reaktorsicherheit, *Schutz der deutschen Kernkraftwerke vor dem Hintergrund der terroristischen Anschläge in den USA vom 11. September 2001*, (*Protection of German Nuclear Power Plants in the Context of the September 11, 2001 Terrorist Attacks in the US*), November 27, 2002.

The NUREG-1465 revised source term is shown in Table 1. The source term is characterized by grouping together fission products with similar chemical properties and for each group specifying a "release fraction"; that is, the fraction of the core radionuclide inventory released from the damaged fuel into the containment building atmosphere. Noble gases include krypton (Kr); halogens include iodine (I); alkali metals include cesium (Cs); noble metals include ruthenium (Ru); the cerium (Ce) group includes actinides such as plutonium (Pu) and the lanthanide (La) group includes actinides such as curium (Cm).

TABLE 1: NUREG-1465 radionuclide releases into containment for PWRs

	Gap	Early In-Vessel	Ex-Vessel	Late In-Vessel
Duration (hrs)	0.5	1.3	2.0	10.0
Release fractions (%):				
Noble Gases (Kr)	0.05	0.95	0	0
Halogens (I)	0.05	0.35	0.25	0.1
Alkali Metals (Cs)	0.05	0.25	0.35	0.1
Tellurium group (Te)	0	0.05	0.25	0.005
Barium, Strontium (Ba, Sr)	0	0.02	0.1	0
Noble Metals (Ru)	0	0.0025	0.0025	0
Cerium group (Ce)	0	0.0005	0.005	0
Lanthanides (La)	0	0.0002	0.005	0

It is important to note that NUREG-1465 is not intended to be a "worst-case" source term. The accompanying guidance specifically states that "it is emphasized that the release fractions for the source terms presented in this report are intended to be representative or typical, rather than conservative or bounding values..."[44] In fact, the release fractions for tellurium, the cerium group and the lanthanides were significantly lowered in response to industry comments. Upper-bound estimates, which are provided in a table in the back of NUREG-1465, indicate that "virtually all the iodine and cesium could enter the containment."[45] And experimental evidence obtained since NUREG-1465 was published in 1995 suggests that the tellurium, ruthenium, cerium and lanthanide release fractions in the revised source term may significantly underestimate actual releases of these radionuclide groups.[46] Thus our use of the NUREG-1465 source term is far from the worst possible case and may underestimate the impacts of credible scenarios.

[44] NUREG-1465, p. 13.
[45] NUREG-1465, p. 17.
[46] Energy Research, Inc., Expert Panel Report on Source Terms for High-Burnup and MOX Fuels, 2002.

We model this scenario in MACCS2 as a two-plume release. The first release begins at the time of vessel breach and containment failure, 1.8 hours after initiation of the accident, and continues over a period of 200 seconds as the containment atmosphere is rapidly vented. The second plume lasts for two hours as core-concrete interactions occur. For simplicity, only the first two hours of the late in-vessel release are included; the last eight hours are omitted, although this late release would likely make a significant contribution to public exposures, given the nearly ten-hour evacuation time estimate for the 10-mile EPZ.

We further assume that the entire radionuclide inventory released from the damaged fuel into the containment atmosphere escapes into the environment through the rupture in the containment. There is little information in the literature about realistic values for the fraction of the containment inventory that is released to the environment. In NUREG-1150, NRC states that "in some early failure cases, the [containment to environment] transmission fraction is quite high for the entire range of uncertainty. In an early containment failure case for the Sequoyah plant ... the fractional release of radioactive material ranges from 25 percent to 90 percent of the material released from the reactor coolant system."[47] A review of the default values of this fraction for the Sequoyah and Surry plants used in supporting analyses for NUREG-1150 indicates that environmental releases ranging from 80 to 98% of the radionuclides in the containment atmosphere were typically assumed. The only case in which significant retention within the containment building occurs is when there is a delay of several hours between the initiation of core degradation and the time of containment failure, which is not the case for the scenario we are considering. Given that we are using only the first three phases of the NUREG-1465 source term, which may underestimate the maximum release of radionuclides like iodine and cesium by 35%, we believe it is reasonable to neglect the retention within the containment building of at most 20% of the radionuclide inventory.

Another plume characteristic that is very important for determining the distribution and magnitude of consequences is the heat energy that it contains. The oxidation of zirconium cladding during core degradation generates a large amount of heat in a short period of time, which can cause the plume to become buoyant and rise. Greater initial plume heights result in lower radionuclide concentrations close to the plant, but wider dispersal of the plume.

It is unlikely that a radiological release at any US PWR would produce a plume as high as the one released during the Chernobyl disaster. Because of the large mass of graphite moderator in the Chernobyl-4 reactor, a hot and long-duration graphite fire caused a very high plume that was responsible for dispersing radionuclides over vast distances. However, at the same time, the exposure and contamination within 50 miles of the Chernobyl site was much lower than it would have been if the plume had not risen so high. This means that the cooler plume that would be characteristic of a core meltdown at Indian Point could actually be a greater threat to the New York metropolitan area than the contamination pattern resulting from the Chernobyl accident might suggest.

---

[47] US NRC, *Severe Accident Risks: An Assessment for Five Nuclear Power Plants*, NUREG-1150, Volume 2, December 1990, p. C-108.

Table 2 shows the two-plume source term for input into MACCS2, adapted from the NUREG-1465 source term in Table 1. The first plume consists of the containment radionuclide inventory at the time of vessel breach (the sum of the first and second columns in Table 1). The second plume consists of the releases generated by core-concrete interactions and a fraction of the late-in-vessel releases (the sum of the third column and one-fifth of the fourth column in Table 1).

TABLE 2: Source term used in MACCS2 model

Plume	Release time (hrs)	Duration(hrs)	Energy release (MW)	Kr	I	Cs	Te	Ba	Ru	Ce	La
1	1.8	0.06	2.8	1	0.4	0.3	0.05	0.02	0.0025	0.0005	0.0002
2	1.86	2	1.6	0	0.27	0.37	0.25	0.1	0.0025	0.005	0.005

The reactor core inventory used was calculated for a representative 3565 MWt PWR at the end of an equilibrium 18-month cycle using the SCALE code, and was then scaled to the Indian Point 2 power rating of 3071 MWt.[48] Since Indian Point 2 operates on a 24-month cycle, the inventory we use here does not represent the peak inventory of the reactor core, which occurs just before refueling.

(b) Meteorology

The calculation of radiological consequences from a severe accident is strongly dependent on the meteorological conditions at the time of the release and for several days afterward. Relevant factors include the wind speed, the wind direction, the atmospheric stability, the height of the mixing layer and the occurrence of precipitation.

The MACCS2 code can utilize a weather sequence of hourly data for a 120-hour period following the initial release. The user has the option to supply a file with an entire year's worth of hourly meteorological data (8760 entries), consisting of wind speed, atmospheric stability class, and precipitation. The program can then calculate up to 8760 results, each corresponding to a release beginning at a different hour of the year. For each set of weather data, MACCS2 can also generate sixteen results by rotating the plume direction into each sector of the compass, repeating the calculation for each plume direction, and then weighting the results with the fraction of the time that the wind blows in that direction (as specified by the user-supplied "wind rose," or set of probabilities that the wind will be blowing in a certain direction at the site). Finally, the code can tabulate the results in a frequency distribution.

[48] Lyman (2001), op cit., pp. 64-66.

The MACCS2 code, like the CRAC2 code before it, has the option to sample a reduced number of weather sequences, based on a semi-random sampling method. The reason for employing a sampling scheme in the past was no doubt the length of computing time needed for each calculation; however, the program runs quickly on modern machines, so there is no need to employ the MACCS2 sampling scheme. In fact, a comparison of the results obtained from sampling, which utilizes about 100 weather sequences, and the results obtained from an entire year's worth of sequences, finds that the peak consequence values in the sampling distribution are 30% or more below the peak consequences over the entire year, if the plume rotation option is not utilized. Thus there is a significant sampling error for peak values associated with the MACCS2 sampling scheme (and presumably the CRAC2 sampling scheme as well).

We were unable to obtain the meteorological data for the Indian Point site needed for input into MACCS2. Instead, we used a meteorological data file for New York City, the location of the nearest National Weather Service weather monitoring station, that was supplied with the original CRAC2 code. This is the same approach that was taken in the CRAC2 Report, which was ostensibly a site-specific study of the 91 sites where nuclear reactors were located or planned, but did not use meteorological data files specific to those sites. Instead, the study used data derived from 29 National Weather Service stations that were "chosen as a representative set of the nation's meteorological conditions."[49] NRC later had to adopt the same approach, using the New York City meteorological data file as a surrogate for Indian Point-specific data in a CRAC2 benchmark exercise, because it was unable to obtain the Indian Point data.[50]

Use of the New York City meteorological data file in lieu of Indian Point site data is a reasonable approximation for the purposes of this report. Two of the most important factors in determining the radiological consequences of a terrorist attack at Indian Point are the wind direction and the precipitation. With regard to the first factor, we use the Indian Point site wind rose to take into account the effect of the variation in wind direction.[51] With regard to precipitation data, since the MACCS2 code only allows for uniform precipitation over the entire evaluation area, the precipitation data set from New York City is just as relevant as data from the Indian Point site for determining the consequences for the New York metropolitan area.

One phenomenon that we cannot fully account for without access to meteorological data specific to the Indian Point site is the coupling between wind direction and wind speed that results from the plant's location in the Hudson River Valley. Wind speeds below a threshold of below 4 meters per second tend to result in plumes that follow the course of the river valley, whereas greater wind speeds produce plumes that are free to travel in any direction and are better approximated by the straight-line Gaussian model. Our use of the

---

[49] R. Davis, A. Hanson, V. Mubayı and H. Nourbakhsh, *Reassessment of Selected Factors Affecting Siting of Nuclear Power Plants*, NUREG/CR-6295, US Nuclear Regulatory Commission, 1997, p. 3-30.
[50] US Nuclear Regulatory Commission, Generic Environmental Impact Statement for License Renewal of Nuclear Plants, NUREG-1437, Vol. 1, Sec. 5.3.3.2.3.
[51] James Lee Witt Associates, *Review of Emergency Preparedness of Areas Adjacent to Indian Point and Millstone*, March 2003, Figure 3-1, p. 21.

Indian Point wind rose accounts for this effect, but to the extent that the distribution of wind speeds in the meteorological data file that we use differs from that at the Indian Point site, the calculations may include some cases that involve unrealistic wind patterns. However, any errors in the distribution resulting from this approximation are not likely to be significant in comparison to the uncertainties associated with use of the straight-line Gaussian model in MACCS2. In any event, it is likely that properly accounting for this effect would result in the channeling of a greater number of slow-moving, concentrated plumes directly downriver toward densely populated Manhattan, thereby increasing the overall radiological impact.

We have also run the calculations using the meteorological data file for the Surry site in Virginia to compare the maximum consequences obtained. We find that the values for peak early fatalities differ by less than 1% and the value for peak latent cancer fatalities differs by less than 5%. We interpret this result as an indication that the peak consequences we found for Indian Point are not due to weather conditions unique to the meteorological data file for New York City.

If Entergy were willing to provide us with data from the Indian Point meteorological monitoring station, we would be pleased to use it to assess whether it would have a significant impact on our results. However, we would expect any impact to be minor.

(c) Protective actions

Another crucial factor in determining the consequences associated with a terrorist attack at Indian Point is the effectiveness of the actions taken to protect individuals within the 10-mile emergency planning zone (EPZ).

The MACCS2 emergency planning model requires the user to input the time when notification is given to emergency response officials to initiate protective actions for the surrounding population; the time at which evacuation begins after notification is received; and the effective evacuation speed. Once evacuation begins, each individual then proceeds in a direction radially outward from the release point at a rate given by the effective evacuation speed.

We have assumed that the time at which the off-site alarm is sounded is coincident with the initiation of core melting; that is, 30 minutes after the attack. It is unlikely that the decision to evacuate could be made in much less time. This choice still provides an interval of 78 minutes between the sounding of the alarm and the initiation of the radiological release, consistent with earlier studies such as the CRAC2 Report.

We have assumed that the delay time between receipt of notification by the public within the EPZ and initiation of evacuation is two hours. This is the default parameter in the MACCS2 code, and is consistent both with earlier estimates of the "mobilization time" and with the most recent ones for the Indian Point site, which found that 100% of the public within the EPZ would be mobilized to evacuate by two hours after notification.[52]

[52] James Lee Witt Associates (2003), op cit., Figure 5-6, p. 96.

The effective evacuation speed was obtained from the mobilization time estimate of two hours and the most recent Indian Point evacuation time estimate (ETE) for good summer weather of 9 hours 25 minutes.[53] Subtracting the two-hour mobilization time leaves a maximum time of 7.42 hours for the actual evacuation. Since the maximum travel distance to leave the EPZ is approximately ten miles, this corresponds to an effective evacuation speed of 1.35 miles per hour, or 0.6 meters per second. The high value for the ETE and the correspondingly low effective evacuation speed reflect the severe traffic congestion within the EPZ that is projected to occur in the event that a crisis occurs at Indian Point requiring evacuation.

Outside of the 10-mile EPZ, the baseline dose calculations assume that individuals will take no protective actions.[54] Although this may not be realistic, we believe that it would be inappropriate to assume otherwise. Since NRC and FEMA do not require that any preparation for an emergency be undertaken outside of the 10-mile EPZ, it would not be conservative to assume that individuals outside of the EPZ would receive prompt notification of the event or would know what to do even if they did receive notification. However, to examine the impact of this assumption on the results, we consider a case where the emergency evacuation zone is extended to 25 miles, and the average evacuation speed remains the same as in the 10-mile EPZ case.

(d) Population distribution

In order to accurately calculate the consequences of a terrorist attack at Indian Point, it is necessary to have the correct spatial distribution of population in the vicinity of the site. MACCS2 has the option to use a site population data file, in which the site-specific population is provided on a grid divided into sixteen angular sectors. The user can specify the lengths of sectors in the radial direction.

Most of our analysis is focused on a circular region centered on the Indian Point site with a radius of fifty miles. The ten-mile EPZ is divided into eleven regions, with divisions at the site exclusion zone (about 0.5 miles), at the one-mile point, and nine successive mile-wide intervals. The region between the EPZ and the fifty-mile limit is subdivided into ten intervals (see Figure 1, below).

Permanent resident population data for the ten-mile EPZ was obtained from the estimates for 2003 generated by KLD Associates for the Evacuation Time Estimate study that it prepared for Entergy.[55] The total number of permanent residents within a ten-mile circular zone around Indian Point in 2003, according to KLD, was 267,099. We have not included the transient population in the region in our calculations, even though it would add another 25% to the permanent population estimate, according to KLD data.

---

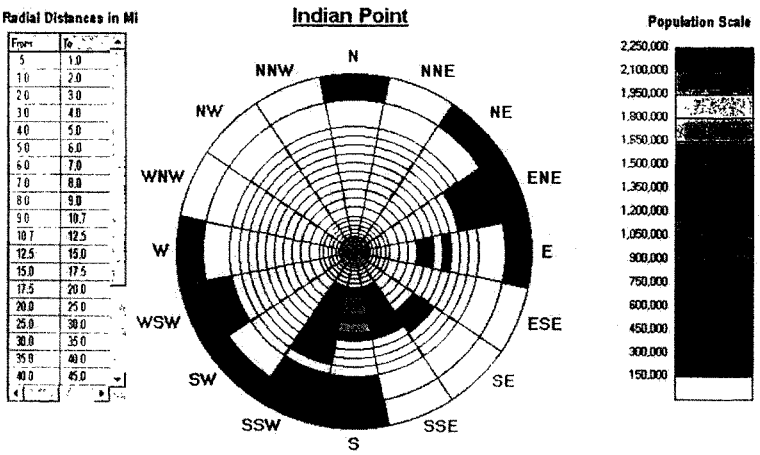
[53] KLD Associates, Inc., *Indian Point Energy Center Evacuation Time Estimate*, Rev. 0 (2003), p. 7-8.
[54] However, the calculation of doses within the EPZ does reflect the impact of "shadow evacuation" of individuals outside of the EPZ, since it uses the KLD Associates evacuation time estimate for the EPZ, which assumes that shadow evacuation occurs.
[55] KLD Associates, Inc. (2003), op cit., p. 3-7.

For the region from 10 to 100 miles from Indian Point, the MACCS2 site data file was generated with the SECPOP2000 code, which is the most recent version of the SECPOP code originally developed by the Environmental Protection Agency and later adopted by NRC for use in regulatory applications.[56] SECPOP2000 utilizes 2000 US Census data to estimate population distributions on a user-specified grid surrounding any location in the United States, drawing on a high-resolution database of over eight million census-blocks. By utilizing the 2000 Census data in SECPOP2000, we have slightly underestimated the population in this region, which appears to have increased by about 1% between 2000 and 2003.

The Indian Point plume exposure EPZ is not in the shape of a perfect circle of ten-mile radius, but includes some regions that are beyond ten miles from the plant. To account for the 38,177 individuals that reside within the EPZ but outside of the 10-mile circular zone (according to KLD estimates for 2003), we used the SECPOP2000 code to determine that an "effective" circular EPZ boundary of 10.68 miles would include the appropriate additional number of permanent residents, and adjusted the MACCS2 grid accordingly.

Figure 1 displays the population rosette generated by SECPOP2000 for Indian Point, out to a distance of 100 miles. The location of New York City is plainly visible on the grid.

FIGURE 1



[56] N. Bixler et al., *SECPOP2000: Sector Population, Land Fraction, and Economic Estimation Program*, NUREG/CR-6525, Rev. 1, Sandia National Laboratories, August 2003.

RESULTS

In this section, we present the results of the MACCS2 simulation of a terrorist attack at IP2, as previously described.

MACCS2 generates results for two distinct periods following a radiological release. First, it calculates the doses to individuals received during the "emergency" phase of the event, defined as the period extending up to the first week following the release. The doses received during this period result from direct exposure to and inhalation of the plume, as well as exposure to plume particles deposited on the ground ("groundshine"). Second, it separately calculates doses received beyond the first week after the release as a result of groundshine, inhalation of resuspended particles, and consumption of contaminated food and water. The first sets of results provided below refer only to the consequences of exposures received during a one-week emergency phase. The economic and long-term health consequences are calculated based on the evaluation of chronic exposures for a period of fifty years following the release, which are dominated by groundshine.

Following the format of the CRAC2 Report summary, our calculation considers several public health and environmental endpoints, including early fatalities, latent cancer fatalities, maximum distance for early fatalities, and total economic costs. The calculations were carried out for each of the 8760 weather sequences in the New York City meteorological data file by rotating the plume direction into each of the 16 sectors of the compass, and then generating a weighted average of the results according to the Indian Point site wind rose. For each endpoint, in addition to the mean of the distribution and the peak value corresponding to the worst-case meteorological conditions encountered during the year, we present the 95th and 99.5th percentile values of the distribution.

The results of the MACCS2 frequency distribution are based on the assumption that the radiological release would occur at random during the year, even though the timing of a terrorist attack most likely would be far from random. As we have previously discussed, one must assume that a terrorist attack intended to cause the maximum number of casualties would be timed to coincide as closely as possible with the most favorable weather conditions. In the case of Indian Point, an attack at night --- the time when a terrorist attack is most likely to be successful --- also happens to be the time when the prevailing winds are blowing toward New York City. Consequently, the mean and other statistical parameters derived from a random distribution are not characteristics of the actual distribution of consequences resulting from a terrorist attack, which would be restricted to a much more limited set of potential release times. A meteorological data set confined to the evening hours would skew the distribution in the direction of increased consequences.

In our judgment, the 95th percentile values of these distributions, rather than the mean values, are reasonable representations of the likely outcome of a well-planned terrorist attack. This choice reflects the fact that the attack time will be largely of the terrorists' choosing, but that some factors will necessarily remain out of their control --- for instance,

the ability to accurately predict precipitation patterns, and the ability to launch an attack exactly as planned.

In the following tables, it is important to note that the peak results in each category do not correspond in general to the same weather sequence. For example, the weather conditions that lead to the maximum number of early fatalities are typically those that involve rainout and substantial deposition of the plume close to the plant, and thus are not the same conditions that lead to peak latent cancer fatalities, which involve rainout of the plume over New York City.

(a) Consequences of radiological exposures during "emergency phase"

Here we consider the consequences of exposures received during the 7-day "emergency phase." We calculate the number of "early fatalities" (EFs) resulting from acute radiation syndrome, both for the residents of the 10-mile EPZ, who are assumed to evacuate according to the scheme described previously, and for the entire population within 50 miles of the plant. Following the CRAC2 Report, we also provide the "early fatality distance," that is, the greatest distance from the Indian Point site at which early fatalities may occur. Finally, we provide an estimate of the number of latent cancer fatalities (LCFs) that will occur over the lifetimes of those who are exposed to doses that are not immediately life-threatening, both for residents of the EPZ and for residents of the 50-mile region.

It is important to note that these estimates are based on dose conversion factors (the radiation doses resulting from internal exposure to unit quantities of radioactive isotopes) appropriate for a uniform population of adults, and do not account for population variations such as age-specific differences. A calculation fully accounting for individual variability of response to radiation exposure is beyond the capability of the MACCS2 code and the scope of this report.

In Table 3, these results are provided for the case in which 100% evacuation of the EPZ occurs, based on the KLD evacuation time estimate and 2-hour mobilization time discussed earlier. Table 4 presents the same information for the case where the EPZ population is sheltered for 24 hours prior to evacuation. Finally, Table 5 presents the results for the extreme case where no special precautions are taken in the EPZ.

In interpreting the results of these tables, one should keep in mind that the MACCS2 code uses different radiation shielding factors for individuals that are evacuating, sheltering or engaged in normal activity. The default MACCS2 parameters (which we adopt in this study) assume that evacuees are not shielded from the radioactive plume by structures, since they are mostly outdoors or in non-airtight vehicles during the evacuation. Individuals who shelter themselves instead of evacuating are shielded to a considerable extent by structures, but may be exposed to higher levels of radiation overall because they remain in areas closer to the site of plume release. The MACCS2 default shielding parameters assume that sheltering reduces doses from direct plume exposure by 40% and doses from plume inhalation by 67%. The relative benefits of sheltering versus

evacuation are obviously quite sensitive to the values of the shielding parameters. Finally, the level of shielding for individuals engaged in "normal activity" falls in between the levels for evacuation and for sheltering, with reductions in doses from direct plume exposure and plume inhalation relative to evacuees of 25% and 59%, respectively.

TABLE 3: Terrorist attack at IP 2, MACCS2 estimates of early fatalities (EFs), latent cancer fatalities (LCFs) and the EF distance resulting from emergency phase exposures, 100% evacuation of EPZ

	Mean	95th percentile	99.5th percentile	Peak
Consequence:				
EFs, within EPZ	527	2,440	11,500	26,200
EFs, 0-50 mi.	696	3,460	16,600	43,700
EF distance (mi.)	5.3	18	24	60
LCFs, within EPZ	9,200	31,600	59,000	89,500
LCFs, 0-50 mi.	28,100	99,400	208,000	518,000

TABLE 4: Terrorist attack at IP 2, MACCS2 estimates of early fatalities (EFs), latent cancer fatalities (LCFs) and the EF distance resulting from emergency phase exposures, 24-hour sheltering in EPZ

	Mean	95th percentile	99.5th percentile	Peak
Consequence:				
EFs, within EPZ	626	2,550	6,370	13,000
EFs, 0-50 mi.	795	3,250	10,200	38,700
EF distance (mi.)	6.2	18	24	60
LCFs, within EPZ	3,770	9,920	12,100	19,400
LCFs, 0-50 mi.	22,700	81,000	192,000	512,000

TABLE 5: Terrorist attack at IP 2, MACCS2 estimates of early fatalities (EFs), latent cancer fatalities (LCFs) and the EF distance resulting from emergency phase exposures, normal activity in EPZ

	Mean	95th percentile	99.5th percentile	Peak
Consequence:				
EFs, within EPZ	4,050	12,600	22,300	38,500
EFs, 0-50 mi.	4,220	13,500	27,300	71,300
EF distance (mi.)	9	18	24	60
LCFs, within EPZ	4,480	10,400	12,500	20,300
LCFs, 0-50 mi.	23,400	82,600	193,000	516,000

A comparison of Tables 3 and 4 indicates that sheltering instead of evacuation results in slightly higher mean early fatalities, but substantially lower 99.5th percentile and peak values. A possible interpretation of this counterintuitive result is that the higher percentile early fatality results for the evacuation case correspond to rare situations in which people evacuate in such a manner as to maximize their radiation exposure (for instance, if they are unfortunate enough to be traveling directly underneath the radioactive plume at the same speed and in the same direction). These situations cannot occur for the sheltering case. Overall, sheltering does appear to substantially reduce the projected number of latent cancer fatalities within the EPZ relative to evacuation, for the default MACCS2 shielding parameters.

A comparison of Table 5 to Tables 3 and 4 indicates that either evacuation or sheltering would substantially reduce the number of early fatalities within the EPZ relative to a case where no protective actions are taken. Also, by comparing Tables 3 and 5, one sees that the number of latent cancer fatalities in the EPZ is considerably lower for the normal activity case than for the evacuation case. There are two reasons for this. First, many evacuees will receive doses that are not high enough to cause early fatalities, yet will contribute to their lifetime cancer risk. In the normal activity case, some of these individuals will receive higher doses and succumb to acute radiation syndrome instead. Second, the MACCS2 default shielding factors give considerable protection to individuals engaged in normal activity compared to evacuees, and may not be realistic.[57]

The peak numbers of latent cancer fatalities for all three cases in the 50-mile zone are disturbingly high, and are more than double the number in the 99.5th percentile. But an examination of the particular weather sequence corresponding to this result indicates that

[57] The protection due to shielding has a bigger impact on the number of latent cancer fatalities, which is a linear function of population dose, than on the number of early fatalities, which is a non-linear function of dose. Shielding would only prevent early fatalities for those individuals whose acute radiation doses would be lowered by sheltering from above to below the early fatality threshold.

the rarity of the event is an artifact of the meteorological data file that we have used, and not a consequence of very extreme or unusual weather conditions for the New York City region. We are not disclosing the details of this weather sequence.

The reader may also notice that the values for the "early fatality distance" for the 95th percentile and above are the same in Tables 3-5, but the mean values are not. This is because the distances for the 95th percentile and above are all greater than 10 miles, so that they are not affected by differences in protective actions that apply only within the 10-mile EPZ.

(b) Doses received by individuals outside of the 10-mile EPZ

It is clear from the previous section that direct exposure to the radioactive plume resulting from a terrorist attack at Indian Point could have severe consequences well beyond the 10-mile EPZ, yet there is no regulatory requirement that local authorities educate residents outside of the EPZ about these risks, or undertake emergency planning to protect these individuals from plume exposures. Therefore, individuals who are now at risk do not have the information that they may need to protect themselves. This is a shortsighted policy, and in fact is inconsistent with government guidelines for protective actions in the event of a radiological emergency.

In this section, we calculate the plume centerline thyroid doses to adults and five-year-old children, and the plume centerline whole-body doses to adults, both at the EPZ boundary and in midtown New York City. (For a given distance downwind of a release, the maximum dose is found at the plume centerline.) We then compare these values to the appropriate protective action recommendations. Thyroid doses are compared to the dose thresholds in the most recent FDA recommendations for potassium iodide administration and whole-body doses are compared to the EPA protective action guides (PAGs) for emergency-phase evacuation. In both cases, the plume centerline doses received to individuals in New York City are well in excess of the projected dose thresholds that would trigger protective actions.

(i) Thyroid doses to children, their consequences, and the need for KI distribution

The statistically significant increase in the incidence of thyroid cancer observed among children exposed to fallout from the Chernobyl disaster leaves little doubt of the causal relationship between the occurrence of these cancers and the massive release of radioactive iodine to the environment resulting from the accident.[58] The effectiveness of widespread distribution of stable iodine in the form of potassium iodide (KI) to block uptake of radioactive iodine in the thyroid was also confirmed in western areas of Poland, where the timely administration of KI was estimated to have reduced peak doses from radioactive iodine by 30%.[59]

---

[58] D. Williams, "Cancer After Nuclear Fallout: Lessons from The Chernobyl Accident," *Nature Reviews Cancer* 2 (2002), p. 543-549.

[59] Board on Radiation Effects Research, National Research Council, *Distribution and Administration of Potassium Iodide in the Event of a Nuclear Incident*, National Academies Press, 2003, p. 58.

In the United States, after resisting public demands for many years, the Nuclear Regulatory Commission finally agreed in January 2001 to amend its emergency planning regulations to explicitly consider the use of KI, and to fund the purchase of KI for distribution within the 10-mile plume exposure EPZs of nuclear plants in states that requested it. This effort accelerated after the September 11 attacks, as more states requested the drug, but even today only fewer than two-thirds of the 34 states and tribal governments that qualify for the KI purchase program have actually stockpiled it. New York State is one of the participants.

Despite a few attempts in Congress after September 11 to require the distribution of KI in areas outside of the plume exposure EPZs, the 10-mile limit remains in effect today, and NRC continues to defend it. In a recent Commission meeting on emergency planning, NRC employee Trish Milligan said that[60]

> "...the [NRC] staff has concluded that recommending consideration of potassium iodide distribution out to 10 miles was adequate for protection of the public health and safety."

Earlier in this briefing, Ms. Milligan provided evidence of the NRC staff's thinking that led to this conclusion:[61]

> "When the population is evacuated out of the [10-mile] area and potentially contaminated foodstuffs are interdicted, the risk from further radioactive iodine exposure to the thyroid gland is essentially eliminated."

These statements again show that NRC continues to use design-basis accidents, in which the containment remains intact, as the model for its protective action recommendations. Although NRC claims that its emergency planning requirements take into account all potential releases, including those resulting from terrorist acts, it clearly is not taking into account catastrophic events such as the scenario being analyzed in this report.

These statements also suggest that NRC is committing the fallacy of using the pattern of radioactive iodine exposure that occurred after the Chernobyl accident as the model for the pattern that could occur here. In the Chernobyl event, the majority of the thyroid dose to children occurred through ingestion of contaminated milk and other foodstuffs that were not interdicted due to the failure of the Soviet authorities to act in a timely manner. However, the food pathway dominated in that case primarily because of the extremely high elevation of the Chernobyl plume, which reduced the concentration of radioactive iodine in the plume and therefore the doses received through direct inhalation.
But as pointed out earlier, the plume from a severe accident at a water-moderated PWR like Indian Point would probably not rise as high as the Chernobyl plume, and the associated collective thyroid dose would have a greater contribution from direct plume inhalation and a lower contribution from milk consumption. In this case, the importance

[60] US NRC, "Briefing on Emergency Preparedness Program Status" (2003), transcript, p. 21.
[61] Ibid, p.19.

of KI prophylaxis would increase relative to that of milk interdiction for controlling overall population exposure to radioactive iodine.

Our calculations clearly indicate that a severe threat to children from exposure to radioactive iodine is present far beyond the 10-mile EPZ where KI is now being made available. In Table 6, we present some results of the distribution for plume centerline thyroid dose to both adults and to five-year-old children at the EPZ boundary and in midtown Manhattan (32.5 miles downwind). In the last column, we provide the projected dose thresholds from the most recent guidelines issued by the FDA for KI prophylaxis.

The thyroid dose to five-year-olds due to I-131 internal exposure was calculated by using the age-dependent coefficients for dose per unit intake provided in ICRP 72, which are approximately a factor of five greater than those for adults. The calculation must also take into account the difference in the rate of intake of air for children and for adults. Children have lower lung capacities than adults, but they have higher metabolic rates and therefore breath more rapidly. The higher breathing rate of children tends to partially offset their lower lung capacity. Data collected by the California Environmental Protection Agency indicates that on average, children consume air at a rate about 75% of that of adults.[62] We have used this figure in our calculation.

TABLE 6: Terrorist attack at IP 2, MACCS2 estimates of centerline thyroid doses to 5-year-olds resulting from emergency phase exposures (all doses in rem)

Location	Age	Mean	95th percentile	99.5th percentile	Peak	FDA KI threshold
Outside EPZ (11.6 mi)	Adult	1,120	3,400	5,850	9,560	10 (ages 18-40) 500 (over 40)
	5 years	3,620	10,900	18,000	32,100	5
Midtown Manhattan (32.5 mi)	Adult	164	429	761	1,270	10 (ages 18-40) 500 (over 40)
	5 years	530	1,310	2,500	4,240	5

The results in Table 6 show that the thyroid doses to 5-year-olds are approximately three times greater than those for adults. This tracks well with information in the World Health Organization's 1999 guidelines for iodine prophylaxis, which states that thyroid doses from inhalation in children around three years old will be increased up to threefold relative to adults.[63]

[62] Air Resources Board, California Environmental Protection Agency, "How Much Air Do We Breathe?", Research Note #94-11, August 1994. On the Web at www.arb.ca.gov/research/resnotes/notes/94-11.htm.
[63] World Health Organization, *Guidelines for Iodine Prophylaxis Following Nuclear Accidents*, WHO, Geneva, 1999, Sec. 3.3.

These results make clear that both 95th percentile and mean projected thyroid doses can greatly exceed the FDA-recommended threshold for KI prophylaxis administration at locations well outside the 10-mile EPZ, for 5-year-old children and for adults of all ages. In Manhattan, KI would be recommended for children and adults under 40, based on the 95th percentile projection.

The health consequences of doses of this magnitude to the thyroid would be considerable. As the 99.5th percentile is approached, the 5-year-old doses are high enough to cause death of thyroid tissue. In fact, they are on the order of the doses that are applied therapeutically to treat hyperthyroidism and other diseases by destroying the thyroid gland. Children with this condition would require thyroid hormone replacement therapy for their entire lives. At lower doses, in which cells are not killed but DNA is damaged, the risk of thyroid cancer to children would be appreciable. According to estimates obtained from Chernobyl studies, a 95th percentile thyroid dose of 1,310 rem to a 5-year-old child in Manhattan would result in an excess risk of about 0.3% per year of contracting thyroid cancer.[64] Given that the average worldwide rate of incidence of childhood thyroid cancer is about 0.0001% per year, this would represent an impressive increase.

These results directly contradict the reassuring statements by NRC quoted earlier. But it is no secret to NRC that such severe thyroid exposures can occur as the result of a catastrophic release. Results very similar to these were issued by NRC staff in 1998 in the first version of a draft report on the use of KI, NUREG-1633.[65] This draft included a Section VII entitled "Sample Calculations," in which the NRC staff estimated the centerline thyroid doses at the 10-mile EPZ boundary from severe accidents using the RASCAL computer code. Table 5 of the draft report shows that the NRC's calculated dose to the adult thyroid at the 10-mile limit ranged from 1500 to 19,000 rem for severe accidents with iodine release fractions ranging from 6 to 35%, for a single weather sequence.[66] In the introductory section, the report states that "doses in the range of 25,000 rad are used to ablate thyroids as part of a therapeutic procedure. Such thyroid doses are possible during severe accidents."[67] NRC's results are even more severe than ours, which were obtained using the NRC revised source term, with a higher iodine release fraction of 67%.

Given NRC's reluctance to provide information of this type to the public, it is no surprise that the Commission withdrew the draft NUREG-1633 and purged it from its web site, ordering the issuance of a "substantially revised document" taking into account "the many useful public comments" that it received.[68] Lo and behold, the second draft of

---

[64] The average excess absolute risk per unit thyroid dose for children exposed to Chernobyl fallout has been estimated 2.1 per million children per rad. D. Williams, op cit., p. 544.
[65] F.J. Congel et al., *Assessment of the Use of Potassium Iodide (KI) As A Public Protective Action During Severe Reactor Accidents*, Draft Report for Comment, NUREG-1633, US Nuclear Regulatory Commission, July 1998.
[66] Ibid, p. 26.
[67] Ibid, p. 6.
[68] US NRC, "Staff Requirements --- Federal Register Notice on Potassium Iodide," SRM-COMSECY-98-016, September 30, 1998.

NUREG-1633, which was rewritten by Trish Milligan and reissued four years later, mysteriously failed to include Section VII, "Sample Calculations," as well as all information related to those calculations (such as the clear statement cited earlier that thyroid doses in the range of 25,000 rad are possible during severe accidents).[69] This took place even though the Commission's public direction to the NRC staff on changes to be incorporated into the revision made no explicit reference to this section.[70] However, it is clear that the expurgated information would be inconsistent with NRC's previous rulemaking restricting consideration of KI distribution only to the 10-mile zone. Even after this exercise in censorship, the Commission still voted in 2002 to block release of the revised draft NUREG-1633 as a final document.

Some insight into the level of understanding of the health impacts of a catastrophic release of radioactive iodine of the current Commission can be found in the statement of Commissioner McGaffigan in voting to delay release of the revised NUREG-1633 for public comment. In his comments, McGaffigan wrote[71]

> "Both WHO [the World Health Organization] and FDA set the intervention level on KI prophylaxis for those over 40 at 5 gray (500 rem) to the thyroid ... Since we do not expect, *even in the worst circumstances*, any member of the public to receive 500 rem to the thyroid, it would be useful for FDA to clarify whether we should plan for KI prophylaxis for those over 40." [Emphasis added.]

This statement is not consistent with what is known about the potential consequences of a severe nuclear accident. Few experts would claim that such high doses cannot occur "even in the worst circumstances," and the NRC's own emergency planning guidance is not intended to prevent such doses in *all* accidents, but only in *most* accidents. Given that the Commissioner presumably read the first draft of NUREG-1633, he would have seen the results of the staff's thyroid dose calculations and other supporting material. There is no discussion in the public record that provides a rationale for Commissioner McGaffigan's rejection of the informed judgment and quantitative analysis of his technical staff.

In 2003, at the request of Congress a National Research Council committee released a report addressing the issue of distribution and administration of KI in the event of a nuclear incident.[72] Most notably, the committee concluded that[73]

> "1. KI should be available to everyone at risk of significant health consequences from accumulation of radioiodine in the thyroid in the event of a radiological incident...

---

[69] US NRC, "Status of Potassium Iodide Activities, SECY-01-0069, Attachment 1 (NUREG-1633, draft for comment; prepared by P.A. Milligan, April 11, 2001).
[70] US NRC, SRM-COMSECY-98-016.
[71] US NRC, Commission Voting Record on SECY-01-0069, "Status of Potassium Iodide Activities," June 29, 2001.
[72] National Research Council (2003), op cit.
[73] Ibid, p. 5.

> 2. KI distribution programs should consider ... local stockpiling outside the emergency planning zone ..."

While the committee did not itself take on the politically sensitive question of how to determine the universe of individuals who would be "at risk of significant health consequences," it did recommend that "the decision regarding the geographical area to be covered in a KI distribution program should be based on risk estimates derived from calculations of site-specific averted thyroid doses for the most vulnerable populations."[74] This is the type of information that we provide in Table 6 (and the type that NRC struck from draft NUREG-1633). We hope that the information in our report provides a starting point for state and local municipalities to determine the true extent of areas that could be significantly affected by terrorist attacks at nuclear plants in their jurisdiction and to make provisions for availability of KI in those regions. Our calculations show that New York City should be considered part of such an area.

However, even timely administration of KI to all those at risk can only reduce, but cannot fully mitigate, the consequences of a release of radioactive iodine resulting from a terrorist attack at Indian Point. The projected dose to individuals who undergo timely KI prophylaxis can be reduced by about a factor of 10. A review of the results of Table 6 shows that doses and cancer risks to many children in the affected areas will still be high even after a ten-fold reduction in received dose. And KI can only protect people from exposure to radioactive iodine, and not from exposure to the dozens of other radioactive elements that would be released to the environment in the event of a successful attack.

(ii) Whole-body doses and the need for evacuation or sheltering

In addition to KI distribution, the other major protective action that will be relied on to reduce exposures following a terrorist attack at Indian Point is evacuation of the population at risk. In Table 7, we present the results of our calculation for the projected centerline whole-body "total effective dose equivalents" (TEDEs) just outside the EPZ boundary and in downtown Manhattan, and compare those with the EPA recommended dose threshold for evacuation during the emergency phase following a radiological incident. As in the discussion of projected thyroid doses and KI prophylaxis, we find that projected centerline TEDEs would exceed the EPA Protective Action Guide (PAG) for evacuation of 1-5 rem at distances well outside of the 10-mile plume exposure EPZ within which NRC requires evacuation planning.

[74] Ibid, p. 162.

TABLE 7: Terrorist attack at IP 2, MACCS2 estimates of adult centerline whole-body total effective dose equivalents (TEDEs) resulting from emergency phase exposures (all doses in rem)

	Mean	95th percentile	99.5th percentile	Peak	EPA PAG
Location					
EPZ boundary (11.6 mi)	198	549	926	1,490	1-5
Midtown Manhattan (32.5 mi)	30	77	131	307	1-5

From the results in Table 7, it is clear that according to the EPA early phase PAG for evacuation of 1-5 rem, evacuation would be recommended for individuals in the path of the plume centerline not only outside of the EPZ boundary, but in New York City and beyond. An individual in Manhattan receiving the 95th percentile TEDE of 77 rem during the emergency phase period would have an excess absolute lifetime cancer fatality risk of approximately 8%, which corresponds to a 40% increase in the lifetime individual risk of developing a fatal cancer (which is about one in five in the United States).

We now examine the potential reduction in health consequences that could result from evacuation of a larger region than the current 10-mile EPZ by considering a case in which the boundary of the plume exposure EPZ is expanded from 10.7 to 25 miles. We calculate the impact of different protective actions in this region on the numbers of early fatalities and latent cancer fatalities among the population within the expanded EPZ but outside of the original 10-mile EPZ. The residents of the expanded EPZ are assumed either (1) to evacuate with the same mobilization time and at the same average speed as the residents of the original EPZ, or (2) to shelter in place for 24 hours and then evacuate. The results are provided in Table 8.

TABLE 8: Terrorist attack at IP 2, MACCS2 95th percentile estimates of early fatalities (EFs) and latent cancer fatalities (LCFs) resulting from emergency phase exposures; 25-mile EPZ

	Normal activity	Evacuation	Sheltering for 24 hrs
Consequence:			
EFs, 10.7-25 mi	664	0	0
LCFs, 10.7-25 mi	19,800	45,700	9,020

These results indicate that evacuation and sheltering are equally effective in eliminating the risk of early fatalities among residents of the 10.7-25 mile region for the 95th percentile case. On the other hand, one sees that evacuation also tends to increase the number of latent cancer fatalities relative to normal activity, while sheltering reduces the number. Thus for this scenario, it appears that sheltering of individuals in the 10.7-25 mile region would be preferable to evacuation of this region for the MACCS2 evacuation and sheltering models we use here. This is consistent with the results we obtained earlier when considering the comparative impacts of evacuation and sheltering of residents of the 10-mile EPZ, again indicating that evacuation tends to increase population doses by placing more people in direct contact with the radioactive plume. However, other models and other shielding parameter choices may lead to different conclusions. We would urge emergency planning officials to evaluate an exhaustive set of scenarios, and to conduct a realistic and site-specific assessment of the degrees of shielding that structures in the region may provide, to determine what types of actions would provide the greatest protection for residents of regions outside of the 10-mile EPZ.

(c) Long-term economic and health consequences

In this section we provide MACCS2 order-of-magnitude estimates of the economic costs of the terrorist attack scenario, the numbers of latent cancer fatalities resulting from long-term radiation exposures (primarily as a result of land contamination), and the number of people who will require permanent relocation. NRC has used MACCS2 to estimate the economic damages of reactor accidents for various regulatory applications.[75]

There is no unique definition of the economic damages resulting from a radiological contamination event. In the MACCS2 model, which is a descendant of the CRAC2 model, the total economic costs include the cost of decontamination to a user-specified cleanup standard, the cost of condemnation of property that cannot be cost-effectively decontaminated to the specified standard, and a simple lump-sum compensation payment to all members of the public who are forced to relocate either temporarily or permanently as a result of the attack. Although simplistic, this model does provide a reasonable estimate of the order of magnitude of the direct economic impact of a successful terrorist attack at Indian Point.

(i) EPA Protective Action Guide cleanup standard

We first employ the long-term habitability cleanup standards provided by the EPA protective action guide (PAG) for the "intermediate phase," which is the period that begins after the emergency phase ends, when releases have been brought under control and accurate radiation surveys have been taken of contaminated areas. The EPA intermediate phase PAG recommends temporary relocation of individuals and decontamination if the projected whole-body total effective dose equivalent (TEDE) (not taking into account any shielding from structures) over the first year after a radiological

[75] US NRC, Office of Nuclear Regulatory Research, *Regulatory Analysis Technical Evaluation Handbook*, NUREG/BR-0184, January 1997, p. 5.37.

release would exceed 2 rem. The EPA chose this value with the expectation that if met, then the projected (shielded) TEDE in the second (and any subsequent year) would be below 0.5 rem, and the cumulative TEDE over a fifty-year period would not exceed 5 rem.

The MACCS2 economic consequence model evaluates the cost of restoring contaminated areas to habitability (which we define as reducing the unshielded TEDE during the first year of reoccupancy to below 2 rem), and compares that cost to the cost of condemning the property. All cost parameters, including the costs of decontamination, condemnation and compensation, can be specified by the user. We employ an economic model partly based on parameters developed for a recent study on the consequences of spent fuel pool accidents.[76] The model utilizes the results of a 1996 Sandia National Laboratories report that estimates radiological decontamination costs for mixed-use urban areas.[77] We refer interested readers to these two references for information on the limitations and assumptions of the model.

The SECPOP2000 code, executed for the Indian Point site, provides the required site-specific inputs for this calculation, including the average values of farm and non-farm wealth for each region of the MACCS2 grid, based on 1997 economic data. These values are used to assess the cost-effectiveness of decontaminating a specific element versus simply condemning it.

Table 9 presents the long-term health and economic consequences calculated by MACCS2 for a region 100 miles downwind of the release, considering only costs related to residential and small business relocation, decontamination and compensation. Since the calculation was performed using values from a 1996 study and from 1997 economic data, we have converted the results to 2003 dollars using an inflation adjustment factor of 1.10. Because of significant uncertainties in the assignments of parameters for this calculation, the results in Table 9 should only be regarded as order-of-magnitude estimates. The reader should note that the latent cancer fatality figures in Table 9 result from doses incurred after the one-week emergency phase is over, and therefore are additional to the numbers of latent cancer fatalities resulting from emergency-phase exposures reported previously in Tables 3 to 5.

---

[76] J. Beyea, E. Lyman and F. von Hippel, "Damages from a Major Release of ^{137}Cs into the Atmosphere of the United States," *Science and Global Security* 12 (2004) 1-12.

[77] D. Chanin and W. Murfin, *Site Restoration: Estimates of Attributable Costs From Plutonium Dispersal Accidents*, SND96-0057, Sandia National Laboratories, 1996.

TABLE 9: Terrorist attack at IP 2, MACCS2 estimates of long-term economic and health consequences, EPA intermediate phase PAG (< 2 rem in first year; approx. 5 rem in 50 yrs)

	Mean	95th percentile	99.5th percentile	Peak
Consequence				
Total cost, 0-100 mi (2003 $)	$371 billion	$1.17 trillion	$1.39 trillion	$2.12 trillion
People permanently relocated	684,000	3.19 million	7.91 million	11.1 million
LCFs, 0-100 mi	12,000	41,200	57,900	84,900
Plume Centerline 50-year TEDE (rem)	4.57	7.04	7.18	7.42

One can see from Table 9 that imposition of the EPA intermediate phase PAG does result in restricting the mean 50-year cumulative TEDE to below 5 rem, but that this limit is exceeded for the higher percentiles of the distribution. Thus for a terrorist attack at the 95th percentile, the subsidiary goal of the EPA intermediate phase PAG is not met.

(ii) Relaxed cleanup standard

In the recent NRC meeting on emergency planning described earlier, NRC staff and Commissioners questioned claims by activists that a severe nuclear accident would render large areas "permanently uninhabitable," arguing that the radiation protection standard underlying that determination is too stringent compared to levels of natural background radiation to which people are already exposed.

For instance, Trish Milligan said that[78]

> "There's been a concern that a radioactive release as a result of a nuclear power plant accident will render thousands of square miles uninhabitable around a plant. It is true that radioactive materials can travel long distances. But it is simply not true that the mere presence of radioactive materials are [sic] harmful... the standard applied to this particular claim has been a whole body dose of 10 rem over 30 years, or approximately 330 millirem per year. This dose is almost the average background radiation dose in the United States which is about 360 millirem per year. Some parts of the country have a background radiation dose two or more times higher than the national average. So in effect this additional 330 millirem dose is an additional year background dose or the difference in dose

[78] US NRC, Briefing on Emergency Preparedness (2003), op cit., transcript, p. 22.

between someone living in a sandy coastal area or someone living in the Rocky Mountains."

Ms. Milligan does not note that her opinion of an acceptable level of radiation is not consistent with national standards, such as the EPA PAGs. The EPA long-term goal of limiting chronic exposures after a radiological release to 5 rem in 50 years corresponds to an average annual exposure of 100 millirem above background, while she implies that even a standard of 330 millirem per year, which would double the background dose on average, is unnecessarily stringent.

However, we can evaluate the impact of weakening the EPA PAGs for long-term exposure on costs and risks. In Table 10, we assess the impact of adopting a long-term protective action guide of 25 rem in 50 years, or an average annual dose of 500 millirem per year. By comparing the 95th percentile columns in Table 10 and Table 9, one can see that relaxing the standard would modestly reduce the post-release cleanup costs by about 25% and drastically reduce the number of relocated individuals by 90%. However, weakening the standard would nearly triple the number of long-term cancer deaths among residents of the contaminated area. Cost-benefit analyses of proposals to weaken long-term exposure standards should take this consequence into account.

TABLE 10: Long-term economic and health consequences of a terrorist attack at IP 2, relaxed cleanup standard (25 rem in 50 years)

	Mean	95th percentile	99.5th percentile	Peak
Consequence:				
Total cost, 0-100 mi (2003 $)	$249 billion	$886 billion	$1.14 trillion	$1.50 trillion
People permanently relocated	118,000	334,000	1.86 million	7.98 million
LCFs, 0-100 mi	36,300	115,000	169,000	279,000

(d) An even worse case

The previous results were based on the analysis of a terrorist attack that resulted in a catastrophic radiological release from only one of the two operating reactors at the Indian Point site. However, it is plausible that both reactors could be attacked, or that an attack on one could result in the development of an unrecoverable condition at the other. Here we present the results of a scenario in which Indian Point 3 undergoes a similar accident sequence to Indian Point 2 after a time delay of just over two hours. This could occur, for example, if Indian Point 3 experienced a failure of its backup power supplies at the time that Indian Point 2 was attacked. Given the loss of off-site power at the same time, Indian Point 3 could experience a small-break LOCA and eventually a core melt, commencing about two hours after accident initiation. We assume that the attackers

weaken the IP3 containment so that it ruptures at the time of vessel failure. In Table 11, we present the results of this scenario for the case of full evacuation of the EPZ.

As bad as this scenario is, it still does not represent the worst case. If any or all of the three spent fuel pools at the Indian Point site were also damaged during the attack, the impacts would be far greater, especially with regard to long-term health and economic consequences.

TABLE 11: Terrorist attack at IP 2 and 3, MACCS2 estimates of early fatalities (EFs) and latent cancer fatalities (LCFs) resulting from emergency phase exposures, 100% evacuation of EPZ

	Mean	95th percentile	99.5th percentile	Peak
Consequence:				
EFs, within EPZ	925	4,660	18,400	34,100
EFs, 0-50 mi.	1,620	8,580	30,900	78,400
EF, distance (mi.)	9.1	21	29	60
LCFs, within EPZ	14,800	42,900	75,100	122,000
LCFs, 0-50 mi.	53,400	180,000	342,000	701,000

CONCLUSIONS

In conclusion, we make the following observations.

1) The current emergency planning basis for Indian Point provides insufficient protection for the public within the 10-mile emergency planning zone in the event of a successful terrorist attack. Even in the case of a complete evacuation, up to 44,000 early fatalities are possible.

2) The radiological exposure of the population and corresponding long-term health consequences of a successful terrorist attack at Indian Point could be extremely severe, even for individuals well outside of the 10-mile emergency planning zone. We calculate that over 500,000 latent cancer fatalities could occur under certain meteorological conditions. A well-developed emergency plan for these individuals, including comprehensive distribution of potassium iodide throughout the entire area at risk, could significantly mitigate some of the health impacts if promptly and effectively carried out. However, even in the case of 100% evacuation within the 10-mile EPZ and 100% sheltering between 10 and 25 miles, the consequences could be catastrophic for residents of New York City and the entire metropolitan area.

3) The economic impact and disruption for New York City residents resulting from a terrorist attack on Indian Point could be immense, involving damages from hundreds of billions to trillions of dollars, and the permanent displacement of millions of individuals. This would dwarf the impacts of the September 11 attacks.

4) The potential harm from a successful terrorist attack at Indian Point is significant even when only the mean results are considered, and is astonishing when the results for 95th and 99.5th meteorological conditions are considered. Given the immense public policy implications, a public dialogue should immediately be initiated to identify the protective measures desired by the entire affected population to prevent such an attack or effectively mitigate its consequences should prevention fail. As this study makes abundantly clear, this population extends far beyond the 10-mile zone that is the focus of emergency planning efforts today.

We hope that this information will be useful for officials in the Department of Homeland Security as it carries out its statutory requirement to conduct a comprehensive assessment of the terrorist threat to the US critical infrastructure, as well as for health and emergency planning officials in New York City and other areas that are not now currently engaged in emergency preparedness activities related to a terrorist attack at Indian Point.

ACKNOWLEDGMENTS

The author would like to thank David Lochbaum, Kenneth Bergeron, Frank von Hippel, Jan Beyea and Lisbeth Gronlund for reading drafts of this report and providing many useful comments and suggestions. All mistakes are the responsibility of the author.

Mr. KUCINICH. I would like to begin with some questions of Mr. Lochbaum. The industry claims to have spent $1 billion since September 11 upgrading nuclear plant security. What does that claim tell you?

Mr. LOCHBAUM. Well, I think it speaks to how unprepared we were on September 11th, because that's money that wasn't spent until afterward. And I also think it reminds me of the billion dollars that was spent fixing safety problems at Millstone or the hundreds of millions of dollars that were spent fixing problems at the Davis-Besse plant.

Mr. KUCINICH. I think they spent about $600 million there and about $1 billion at Indian Point to restore plants to a safe level. So how many billions will it take to increase security, in your estimation, to adequate levels?

Mr. LOCHBAUM. I don't think it's a question of money. I don't think there's that much money left to be spent. I think it's more of an attitude question that this subcommittee has explored. I think it's more of a focus and just getting serious about it, more so than the dollar amount, that is preventing it so far. I think the fact that they have been able to do as much as they have behind closed doors is the biggest barrier to getting it done right.

Mr. KUCINICH. And, in your thinking about this, have you thought about some alternatives to this such as solar, wind? Has the NRC and, to your understanding, or the industry spent any money for security at these facilities?

Mr. LOCHBAUM. Well, if you look at the $1 billion that the industry has spent on upgrading nuclear power plant security and compare that to the amount that's been spent upgrading at wind farms or other renewable technology, if it's been $100, it would probably high.

Mr. KUCINICH. Would these wind farms be less of a target?

Mr. LOCHBAUM. There's no real hazard there, so there's no real need to provide $1 billion of security to something that is not a hazard to the American people.

But the real question is—and it is something beyond me to answer—but is it really worth spending $1 billion protecting Americans or is it better to spend the $1 billion more productively in providing an energy technology that doesn't provide that risk to ourselves?

Mr. KUCINICH. Well, you make a series of recommendations in your testimony how to improve physical security at nuclear plants. Do you want to offer to this committee what recommendations you think should be implemented first?

Mr. LOCHBAUM. If I had one to pick from, it would be the spent fuel pool issue, in reducing the threat from spent fuel. Right now, from both a safety standpoint and a security standpoint, we are doing that wrong.

Mr. KUCINICH. Let me ask you something. Why this issue of the transfer of the cask?

Mr. LOCHBAUM. Right.

Mr. KUCINICH. Why has this transfer of spent fuel into dry cask not been done before now?

Mr. LOCHBAUM. We started doing it in 1986 in this country. At that time, the casks that we were using could only be used for stor-

age, not for transport. So there was a reluctance to transfer things into dry cask that would then have to be handled twice. Nowadays, the casks that we have can be used for storage and transport. You are going to have to put it in the cask eventually. Why not do it now where it improves safety, it improves the security, and it doesn't affect the cost that much?

Mr. KUCINICH. Thank you, just have another question for Mr. Fertel.

Mr. SHAYS [presiding]. You may have as much time as you want.

Mr. KUCINICH. Earlier you heard it brought into the discussion, the situation at Davis-Besse. Would you characterize—are you familiar with it?

Mr. FERTEL. Yes, I am.

Mr. KUCINICH. Would you say the events surrounding Davis-Besse are an exception or the rule in the nuclear industry?

Mr. FERTEL. I would say they were the exception, and it was an unacceptable exception.

Going back to questions asked by this committee about lessons learned, following the Davis-Besse event there was a significant lesson learned in our industry resulting in a major materials initiative to make sure that we are looking at materials degradation everywhere in the plant in a much more systemic and integrated way.

It's been a very painful lesson for FirstEnergy. It's been a very painful lesson for FirstEnergy, and it's been a very painful lesson for people like yourself, I am sure. It's actually turned out, for the rest of our industry, something that has focused us much better looking at materials issues. We were spending almost $60 million a year looking at materials issues, so it wasn't something being ignored.

Mr. KUCINICH. So you have learned something from what has happened.

Mr. FERTEL. Yes, sir.

Mr. KUCINICH. In the end, you think it will result in more sensitivity from these other plants and in the long run there is good that might come from it.

Mr. FERTEL. There is good that's come already, sir, as far as a much better technical look at this, a much stronger and integrated look at the analyses, the inspections that you need to do, and clearly a much better awareness at every plant of the importance and the safety culture aspects related to it. So, yes, sir.

Mr. KUCINICH. Just a final question which you are anticipating. What about these force-on-force exercises? I mean, shouldn't they contain an element of surprise?

Mr. FERTEL. Well, yes, sir.

Mr. KUCINICH. Are you surprised that they did?

Mr. FERTEL. Again, I think people have talked about the DOE exercise a lot. And let's talk about the new requirements NRC has put in for force-on-force exercises and deal with that and let me talk about the Wackenhut issue, since everybody else has mentioned it so far today.

Mr. KUCINICH. OK.

Mr. FERTEL. We used to do force-on-force exercises at nuclear power plants every 7 years. NRC now will come in and they will

evaluate them at least once every 3 years, but that's just part of the story. They have established standards for what the training needs to be for not only the people that protect the plant but for the adversaries, the qualifications for not only the people that protect the plant but the adversaries.

We are going to be doing multiple force-on-force exercises, in addition to normal training and gun firing and things like that—real force-on-force exercises, every plant every year. I can't tell you how many, which is silly to me, but it is safeguards, and I don't know why. I think that's a silly thing.

When we in the industry looked at this, we said, the way we should do this, the same model for training operators. We should go to a systemic approach to training, which is a very rigorous way to do it. Make sure we have the discipline in our system for security activity just like we do for operator training. That's what we are doing.

We also looked at and we said, the way these force-on-force exercises are done—and, Mr. Turner, I think said that, at DOE, the Secretary had formed a special adversary group. Those are DOE people. They are not outsiders. OK.

When the U.S. Army does their war games, they use the U.S. Army. OK. They don't bring the Russians in. You know, they don't bring in other bad guys. They do it professionally.

Mr. KUCINICH. From what I understand, if I may, they don't describe information ahead of time as to——

Mr. FERTEL. I will get the information. The information that is described ahead of time in force-on-force exercises now.

You do need to know when they are going to do it at the site. Because, while you are doing an exercise, there's real guys with real guns protecting the site. So people need to know that you are going to do an exercise at that site. That's known.

Outside of that, they don't know. They don't go—I don't know what happened at the Y–12 facility. It's the first I heard of it, because I don't follow the DOE stuff where they said what facility they were going to attack.

But, as Luis Reyes said, this scenario that they do on the attack and the way NRC is doing this is being developed by NRC. They decide what the attack is, whether it's to go for spent fuel. The adversaries know that. They get help from an insider. The defensive guys don't know this.

Mr. KUCINICH. So Wackenhut then, the guy wouldn't cheat at mock drills at NRC facilities, but we have something on the record that suggests that at DOE facilities it might be a little different.

Mr. FERTEL. I don't know whether Wackenhut would cheat at anything. I think human beings cheat. Human beings make mistakes, and human beings do things they shouldn't.

Mr. KUCINICH. Well——

Mr. FERTEL. The people that we have running this CAF team, OK, the people that are doing this Composite Adversary Force, the three top people that are running that basically are all Special Forces, OK? They never worked for the industry before. The project manager has 10 years as a Ranger. One of the team leaders was a team leader for the Delta Force. The other team leader is a special ops guy who ran a whole bunch of guys that did all types of

things like snipers and everything else. These guys want to win, OK? They are out there to do the best job they can and to win.

On our side—and I think this gets lost in almost every discussion about nuclear energy. I think it's important. I certainly feel as passionately about this, Congressman, as you do about your Davis-Besse experience. I know a lot of people that work at the plants. I find it insulting personally when their integrity is challenged all the time, OK?

I think David Lochbaum offers a lot of positive things that have helped us in a number of areas of safety, and I may agree with some insecurity issues, some of which are being dealt with. That's helpful. But the people at the plants who work there—but who do you think gets killed first if terrorists attack and win? They do. OK? Who do you think gets hurt if something happens at a plant and something happens offsite? Their family, their friends and their neighbors. So the implication that they don't care I think is actually really wrong.

Now that doesn't mean you don't make mistakes. It doesn't mean you can't do things better. I think that's one of the things we really want to do. We talked about sleeping guards and so forth and what happens with energy. What happened at sites where that happened is they fired them.

Mr. KUCINICH. When you said the implication they don't care, who are you speaking of?

Mr. FERTEL. Well, I mean, that's the way most of the discussion has gone, to be honest. You know, well, if NRC isn't doing this, the plants wouldn't; and, gee, the guys at the plants don't care unless David Lochbaum or Alex Matthiessen are involved.

I am not saying they shouldn't be involved. All I am saying is that the people that work at those plants care as much about safety and security as anybody who sits up here talking with us or talking to you. I think we need to understand that.

Mr. KUCINICH. I don't know that there is anybody on this committee that would dispute that.

Mr. FERTEL. I am glad to hear that.

Mr. KUCINICH. Except, you know, for one qualification. And that is that you know and I know that all of these people who care so much about doing the right job for themselves, their co-workers, their family or community, there's a few people that make the decision. Now, granted, my experience is greatly informed by something in my own backyard. I understand that.

Mr. FERTEL. I understand that.

Mr. KUCINICH. When we know that photos in this hole in the reactor head were kept out of the file deliberately, when we know this thing wasn't reported, when we know when the NRC had full information they didn't move forward to act on it, I know that, too. So I am not using that to impugn the whole industry.

I have given you an opportunity to acquit the industry, and you did. But, you know, I am saying that when you have one problem like that, because we are talking about nuclear power plants, it requires the utmost in terms of accountability, and that's what this committee is about.

I want to thank the gentleman and thank the Chair for his indulgence. Thank you.

Mr. SHAYS. I am going to, at this time, turn to the professional staff to ask some questions.

Mr. CHASE. Thanks.

Mr. Fertel, a quick question. NRC says that it's going to take 3 years to implement and to test the new security plans. You are saying that there will be force-on-force exercises every year. What goes into developing these force-on-force exercises, having seen a number of them. The question I have is, has any thought been given to prioritizing these force-on-force exercises? There are a number of plants that are in the more densely populated areas. Indian Point is one example. Has any thought been given in terms of prioritizing where and when we should do these exercises?

Mr. FERTEL. First of all, NRC is making all those decisions. The plants have no idea until a set period before the exercise that the planning can be done. So if I'm at the end of next year, I don't know now, I'll know within a few weeks because they've got to do planning.

There has been some of what you've asked for already done. Because NRC has been doing a pilot and a transitional force-on-force exercise program for the last 2 years; and over the latter part of this year, it's been testing the new design basis threat as part of it. Even though you don't have everything necessarily in place, you knew what you were going to do and you were able to test it. And what they have chosen—for instance, Indian Point. Indian Point has already had both a force-on-force and an integrated response and an emergency planning exercise.

So I think the NRC has attempted to do some of that.

My understanding—and, again, I'm giving you kind of an arm's length because they make the decision—is that there is probably about 30 sites that haven't gone through the force-on-force, and those are the ones that haven't gone through the transitional period in the last year and a half or two. Those are the ones that they would pick from for the first year starting November of this year, and I think they will prioritize their—based upon looking at factors like where the site is, when was the last time they actually exercised, and things like that. So, to some degree, it's being done already.

Mr. CHASE. But a concern could be that the force-on-force exercises that were done or have been done to date are under the old DBT, not under the new DBT.

Mr. FERTEL. Some were.

Mr. CHASE. So what I'm asking is, under the new DBT, we know that it's stronger, supposedly stronger. Have they given any thought to prioritizing?

Mr. FERTEL. They haven't shared that with us. And to be honest, they don't want to share it with us because they don't want to give the sites much lead time in knowing what's going on.

Now, again, starting in November, starting actually later this year, every site will start doing their own force-on-force exercises as part of what they have to do, and it's more than one a year per site, absent NRC. And, as I think Roy Zimmerman said, they will probably have their residents and others observing lots of those. And my guess is they could do that, because every site, whether it's an Indian Point site or it's North Anna, will be doing them as

part of their normal routine annual training that they're going to have to do. But I don't have an explicit answer to your question because NRC controls that.

Mr. CHASE. Do either of the other witnesses want to comment? OK.

Mr. Matthiessen, I'm curious. On what basis do you conclude the NRC-revised DBT is too low?

Mr. MATTHIESSEN. Well, on what basis do I—well, just because the DOE is requiring greater DBT and also because I think in a post September 11 world we have to be thinking in terms of the most sophisticated, multi-directional suicidal attacks. And from what I know—and I obviously can't repeat it here—the NRC has only bumped up its DBT marginally, and I think there really needs to be a much more serious level.

Mr. SHAYS. Let me just ask you, though. I mean, basically, why would you be in a position to know what the DBT was?

Mr. MATTHIESSEN. Why would I be in a position to know what it is?

Mr. SHAYS. It's not public.

Mr. MATTHIESSEN. Well, I don't know specifically what it is. I have an indication or a sense of what it is.

Mr. SHAYS. So it's admittedly third-hand concerns.

Mr. MATTHIESSEN. It is. But I take it on pretty good——

Mr. SHAYS. You all tend to get your information fairly accurately, but I was just curious.

Mr. MATTHIESSEN. I would just love to make a comment in response to Mr. Fertel, if I could. I just want to mention that he mentioned the force-on-force drill at Indian Point and the emergency planning exercises that were done earlier this summer. I would just suggest that if those are any indication of what the rest of the industry can look forward to, then I think we are in trouble, and I think that the public should be very, very concerned.

In the case of the emergency planning exercise that was done, the NRC, in what looked like a PR move more than a serious test of emergency planning, did conduct a terrorist mock attack on the plant. But, unfortunately, the test didn't involve any release of radiation whatsoever. So as far as I was concerned, they might as well have been testing the security or emergency planning around a Wal-Mart. I mean, the whole point of doing these emergency plans is because nuclear reactors are a special case, they contain materials that are very, very dangerous, and what we need to think about is a worst-case scenario, and a worst-case scenario does involve the release of radiation.

And, likewise, for the force-on-force test, again, they tend to get advance notice, way in advance. The operators, from what we've heard again from security guards inside the plant, spent a lot of time and money beefing up security to abnormal levels in anticipation of the actual day. The attacks happen in day light over prescribed routes. From what we understand, the mock terrorists were not trained at terrorist levels and not equipped with the kind of weaponry that terrorists would likely have.

So, again, I think that the integrity of these exercises is not what it needs to be if we are serious about truly testing the ability of

these plants to repel a terrorist attack and to evacuate and protect people in the event of a terrorist attack.

Mr. SHAYS. If you could just respond to that last point.

Mr. FERTEL. Just on the force-on-force at Indian Point, I was not there, so I can't verify; and I don't think Alex was there, either. But I do know that one of the reasons I heard that they do do night exercises as part of force-on-force, it's pretty routine. I think at Indian Point they made a conscious decision because of the terrain and the danger that they were not going to do it as part of this pilot program when they were doing it, and I understand that was a very conscious decision to avoid personnel injury at the point. But night exercises are part of force-on-force.

Coming up November 1st, when these orders are effective, all the adversaries will have to meet the standards both for their capability and their fitness that the NRC has set. And that's pretty good standards. And, again, that's a major improvement over before September 11, to be honest, and as will the defenders. So I would expect, Alex, that you will see—I can only go by what you said on Indian Point, but you will see improved force-on-force at Indian Point as they start their exercises.

Mr. MATTHIESSEN. I hope so, but we may not see the results for another 3 years.

Can I just ask a question of Mr. Fertel?

Mr. SHAYS. No.

Mr. MATTHIESSEN. Sorry.

Mr. SHAYS. That's all right. You can ask us a question if you would like. What's the question you would like us to ask him?

Mr. MATTHIESSEN. Well, I would just like to ask why—what is the industry and the NRC's response for not instituting what we see as pretty straightforward measures that wouldn't even cost the industry that much that would add an enormous measure as far as we have been led to believe.

Mr. SHAYS. Such as?

Mr. MATTHIESSEN. A couple of the passive systems, barriers that I mentioned in my testimony, the Dunlop barriers and the Beamhenge, these are ways that you would really—you'd go a long way toward protecting these facilities and——

Mr. SHAYS. We will make sure that we have a dialog about that.

Mr. MATTHIESSEN. OK.

Mr. CHASE. Mr. Fertel, how optimistic are you that the industry—according to GAO and the NRC, they are saying that the implementation of the security plans are going to take place by the end of October of this year. How confident are you that's going to actually happen?

Mr. FERTEL. As of 2 weeks ago, everybody was on schedule to be able to meet the requirements of the orders by October 29th. There's some issues where people may not have the picture that the chairman liked of the bullet-resistant enclosure that protects the officers. There are some plants that may have some problems in getting deliveries of some of those and will have to take other actions, and that's mainly because our soldiers in Iraq and our Defense Department and the DOE are getting priority. There's only two sources of steel for those, apparently; and our guys get bumped

a bit on that. But, otherwise, we are going to be ready on October 29th.

Mr. CHASE. And, last, Mr. Matthiessen, would you share with us your thoughts or give us the status on the—if you can recall. The concerns regarding evacuation plans in New York and Connecticut.

Mr. MATTHIESSEN. I mean, again, what concerns me so much is that the FEMA used to have a policy of requiring certification of the plans by the four counties that surround the plant as well as the State. But a couple years ago, after the Witt report came out and showed pretty conclusively that this plan couldn't work in the event of a terrorist attack on the plant, especially—or, sorry, a radioactive release, especially in the case of a fast-breaking release, these counties became very uncomfortable and became convinced that it really wasn't possible to evacuate or even shelter people in place of a level that would be satisfactory, and so they withdrew that certification, as did the State emergency management office.

And the FEMA came out, as you probably know, last August and just rubber-stamped the emergency plan without any evidence—not providing any evidence—this shouldn't be safeguards information, most of it anyway—without any evidence or analysis upon which they base that conclusion. And, of course, the NRC came out and rubber-stamped it a half an hour later, on a Friday in late July. And this is kind of typical of these agencies.

And, again, I think you don't have to be a James Lee Witt that, given the road congestion, given the population densities, there is just no way that you could realistically evacuate that area or shelter people in place.

Second, I do want to make a comment on the——

Mr. SHAYS. I'm sorry, I need to interrupt you.

Mr. MATTHIESSEN. I'm sorry.

Mr. SHAYS. I have a need to be sitting at a desk at 2 in order to not lose my place in another committee hearing. So, if that's all right, let me just go on and ask.

What I'm wrestling with, Mr. Lochbaum, is—first of all, Mr. Fertel, what I'm the wrestling with is that I think the industry needs to do a better job, as much as you point out it was one of the most secure industries before September 11, because I think that we are going to have to have a very significant debate about the future of nuclear energy. And I wrestle as an environmentalist with the fact that, if I want to get at greenhouse gases, is there a role that nuclear energy has to play.

Right now, Millstone's one, two, and three are about 50 percent of Connecticut's—based on your testimony, and it used to be more when we had the Yankee plant plus one, two, and three—you know, we were oversubscribed. But tell me how you sort out, Mr. Lochbaum. Do you think nuclear energy simply can't be expanded at all?

Mr. LOCHBAUM. I guess we view nuclear energy as providing the bridge to the future, with renewable energy technologies and improved energy efficiency being that future. But that future is, quite frankly, not here today. So we think that the safe operation of existing plants, until the—as they reach in their normal lifetimes they get replaced by better technologies of the 21st century technologies would be our druthers.

Mr. SHAYS. This spent fuel is a huge concern to me. And, you know, I see them at the facility on the Hudson River, you know, saw the pool where they are at and so on. And they were in the contained area, I believe, is my recall. But we just are collecting more and more of this. Mr. Fertel, how do you wrestle with that?

Mr. FERTEL. Well, I think Congress clearly has a good role to play in moving the ball forward on Yucca Mountain, funding it appropriately, providing the oversight to DOE to make sure they do it appropriately and dealing with the issues around it will move that ball forward. I think, in the interim, clearly you're going to try and do everything you can and are doing everything to manage it safely from a security standpoint, NRC has issued advisories to the plants on what they can do to improve security.

Mr. SHAYS. Let me ask you this. How is it that we have been able to increase production when we haven't added a plant in 30 years?

Mr. FERTEL. Well, we actually have added a lot of plants in the last 30 years. We just haven't ordered a plant in that period.

Mr. SHAYS. We haven't what?

Mr. FERTEL. We haven't ordered a new one, but we've added about 50 plants since 1980. But the way we have increased it in the decade——

Mr. SHAYS. We've had 50 plants since 1980?

Mr. FERTEL. Yeah.

Mr. SHAYS. How many have we had since 1990?

Mr. FERTEL. As far as real plants, concrete and steel? Two, I think.

Mr. SHAYS. OK.

Mr. FERTEL. But we have added the equivalent of 19 since 1990 in improving output from the plants, operating them better, doing a thing that we call uprates, where you can either improve the turbine or you can improve something on the reactor, on the reactor side to get more power out of it. And we have added two plants. So we've added about 19,000 megawatts since 1990 in kilowatt hours out.

Mr. SHAYS. Do you all want to quickly speak to this issue of citations and whether they have to respond in writing or so on? I mean, is this of concern? Or are we more concerned than we should be?

Mr. LOCHBAUM. As Mr. Reyes said, it's consistent with how they deal with safety issues. So it's the same approach. I also go back to what Mr. Zimmerman said. They are piloting the new significance determination process.

Mr. SHAYS. And that's a good thing.

Mr. LOCHBAUM. Well, it depends on how it comes out. It's a trial run now. But that could—depending on how that outcome is, could go further to better defining that line between what gets reported and what gets followed up, what the plant owners do and what the NRC does. I'm comfortable with that. If there is a better way of doing it, I'm open to that. But I bought into the process and I'm comfortable with it the way it is.

Mr. FERTEL. I think an aspect that maybe could help your comfort level—because you clearly weren't comfortable with it, listening to the discussion, is that I think the impression when they say

they are doing a sample makes it sound like, oh, my God, they're just choosing a few. When they're doing the sample, they are doing a sample in security, they are doing a sample in safety, they are doing samples in other areas. And what they are looking for, in all honesty, is to see if there is any sort of a systemic breakdown in the corrective action program that the plant uses. And if they see a breakdown, well, then it's a whole other ball game for the NRC to come in and basically do major inspections. So they want your processes to work; and, if they work, they are comfortable.

Mr. SHAYS. OK. I am going to adjourn.

Actually, there is one other question. If staff's waiting for me—I am going out that door and I'm hustling. I have a better feeling of knowing the NRC is present every day. Are we underutilizing those folks? If you don't know, that's another issue.

Mr. LOCHBAUM. We were concerned that—several years ago, the NRC changed its policy, like in 1997, 1998. They used to have more NRC resident inspectors, more people onsite. As part of a budget-cutting move, they removed some of the people from that onsite presence. That contributed to the problem that Davis-Besse—that Representative Kucinich is concerned about.

Mr. SHAYS. But it seems to me that they could be doing followup. I mean, evidently, they have prescribed things they should do.

Mr. LOCHBAUM. It's hard when there's so few of them. If they went back to the levels they had 5, 6 years ago, they could do more because there were more people there.

Mr. SHAYS. Well, if you have two and you add one more, that's three. That's a 50 percent increase. Maybe even that would be beneficial.

Mr. LOCHBAUM. It couldn't hurt.

Mr. SHAYS. I'm sorry. I have a feeling there's some other things we could say, but it's been a long day, and it's been a very helpful day, and I appreciate all your contribution. So, we are going to call this hearing closed. Thank you.

[Whereupon, at 2:07 p.m., the subcommittee was adjourned.]

○