03-4313

UNITED STATES COURT OF APPEALS for the SECOND CIRCUIT

----------X

Riverkeeper, Inc.,

Petitioner,

- against -

SAMUEL J. COLLINS, Director, Office of Nuclear Reactor Regulation; DR. WILLIAM TRAVERS, Executive Director for Operations of the Nuclear REGULATORY COMMISSION; the UNITED STATES OF AMERICA; ENTERGY NUCLEAR INDIAN POINT 2 LLC; ENTERGY NUCLEAR INDIAN POINT 3, LLC; and ENTERGY NUCLEAR OPERATIONS, INC.

Respondents.

----------X

On Petition for Review of a Decision of the Nuclear Regulatory Commission

Joint Appendix: Volume 3 of 3

Pace Environmental Litigation Clinic, Inc.
78 North Broadway
White Plains, New York 10603
914-422-4343
Attorney for Plaintiff-Appellant

Of Counsel:
Karl S. Coplan

Legal Interns:
Nicolette Witcher
Joseph Vinciguerra

David A. Cummings
Office of the General Counsel
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
301-415-1520
Attorney for Federal Respondents

Jay E. Silberg, Esq.
David J. Cynamon, Esq.
Matias F. Travieso-Diaz, Esq.
Shaw Pittman, L.L.P.
2300 N Street, NW
Washington, D.C. 20037
Attorney for Entergy Respondents

TABLE OF CONTENTS

Volume 1

Certified Index of the Record.....1

Letter From Samuel J. Collins to Alex Matthiessen Enclosing Director's Decision.....12

Letter Secy to Matthiessen Informing Commission Declined Any Review; Decision Became Final Agency Action.....50

Section 2.206 Request for Emergency Shutdown of Indian Point Units 2 and 3.....52

Exhibit 1:U.S. Conference of Mayors, "If U.S. City/County Metro Economies Were Nations".....80

Exhibit 2: Daniel Rubin, "Nuclear Terrorism Threat Growing," (Knight Ridder Foreign Service).....81

Exhibit 3: CNN, "Threat at Three Mile Island Closes Airports,".....84

Exhibit 4: International Atomic Energy Agency, "Calculating the New Global Nuclear Terrorism Threat".....85

Exhibit 5: Eric Pianin and Dan Eggen, "Preparations Stepped Up for Possible New Attacks".....90

Exhibit 6: Lara Mansnerus and Judith Miller, "Terrorist Details His Training in Afghanistan).....94

Exhibit 7: Nicholas Rufford, David Leppard and Paul Eddy, "Nuclear Mystery: Crashed Plane's Target May Have Been Reactor".....98

Exhibit 8: CNN: "FAA Restricts Flights Near World Series, Nuclear Plants".....102

Exhibit 9: William Branigin, "In Afghan Jail, a Terrorist Who Won't Surrender".....106

Exhibit 10: NRC, Press Release No. 01-112, "NRC Reacts to Terrorist Attacks".....112

Exhibit 11: NRC Report, "Technical Study of Spent Fuel Pool Accident Risk At Decommissioning Nuclear Power Plants".....115

V.L. Sailer Et Al. "Severe Accident In Spent Fuel Pools In Support of Generic Safety Issues 82" NUREG/CR-4982.....203

Exhibit 12: Roger Witherspoon, "Indian Point Chief: Plant Safe From Possible Attack".....360

Exhibit 13: Vibeke Laroi, "Nuclear Plant Scare Adds to U.S. Security Jitters".....362

Exhibit 14: Douglas Pasternak, "A Nuclear Nightmare".....365

Exhibit 15: Paul. L. Leventhal, Commencement Address to the Class of 2001 at Franklin & Marshall College.....369

Exhibit 16: Shawn Cohen, "NRC Flags ConEd With Red Tag for Indian Point".....376

Sandia Labs, NRC, "Calculation of Reactor Accident Consequences" (1982) (CRAC-2 Report).....380

Exhibit 17: "At Indian Point, A History of Nuclear Power, Problems and Controversy".....392

Declaration of 20 December 2001 By Gordon Thompson in Support of a Petition by Riverkeeper, Inc.....398

Letter From Samuel Collins (NRC) to Alex Matthiessen (Riverkeeper) Acknowledging Receipt of Riverkeeper's 2.206 Petition and Denying Immediate Closure of Indian Point 2 and 3.....435

Licensee's Response to Riverkeeper, INC.'s Section 2.206 Request for Emergency Shutdown of Indian Point Units 2 and 3.....442

Volume II

NRC Supplemental Inspection Report No. 05000247/2001-002, Indian Point Unit 2 486

AEC Regulatory Guide 1.78 603

NRC Inspection Manual, Inspection Procedure 81110, Operational Safeguards Response Evaluation.....613

Letter from NRC Chairman Richard Meserve to Senator James Jeffords.....624

Letter from G. Scott Barber (NRC) to J. Barret (Entergy) (Enclosing NRC Inspection Report 50/286/01-09).....638

NRC Office of Nuclear Reactor Regulation, Directive 8.11, "Review Process for 10 C.F.R. 2.206 Petitions".....664

"Malevolent Use of Vehicles at Nuclear Power Plants" 59 Fed. Reg. 38889.....704

"Final Rule: Physical Protection for Spent Nuclear Fuel and High-Level Radioactive Waste" 63 Fed. Reg. 26955.....724

NURGE-0800, Section3.5.1.6, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants".....741

NURGE-0654/FEMA-REP-1 (Rev. 1), "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Preparedness in Support of Nuclear Power Plants.".....749

NRC Inspection Report 95000286/2000-10.....902

"Evaluation of Aircraft-Crash-Hazards Analysis for Nuclear Power Plants," NUREG/CR-2859.....912

Proposed Director's Decision Under 10 CFR 2.206.....926

Riverkeeper's Comments on May 16, 2002 Proposed Director's Decision on Riverkeeper's November 8th Petition 2.206 Request for Emergency Shutdown of Indian Point Units 2 and 3.....951

Volume III

Exhibit A: National Research Council, "Making the Nation Safer" The Role of Science and Technology in Countering Terrorism" 976

Exhibit B: Associated Press, "Planes Often Enter Prohibited Air".....1004

Exhibit C: ABC News, "Subways, Scuba Divers and Landmarks".....1008

Exhibit D: CBS News, "Dozens of Airport Workers Arrested".....1012

Exhibit E: CBS News, "Airport Security Gets an 'F'".....1014

Nuclear Control Institute, "The Impact of Nuclear Plant Shutdown on Severe Accident Consequences".....1016

Rep. Edward Markey, Security GAP: "A Hard Look at the Soft Spots in our Civilian Nuclear Reactor Security".....1019

NRC, Regulatory Issues Summary (RIS) 2001-16, "Update of Evacuation Time Estimates".....1036

MAKING THE NATION SAFER

THE ROLE OF SCIENCE AND TECHNOLOGY IN COUNTERING TERRORISM

Committee on Science and Technology for Countering Terrorism
NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

000976

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

Support for this project was provided with institutional funds.

Library of Congress Cataloging-in-Publication Data

Making the nation safer : the role of science and technology in countering terrorism / Committee on Science and Technology for Countering Terrorism. National Research Council.
p. cm.
ISBN 0-309-08481-4 (perfect)
1. Terrorism—Prevention—Technological innovations. 2. Terrorism—United States—Prevention. I. National Research Council (U.S.). Committee on Science and Technology for Countering Terrorism.

HV6431 .M354 2002
363.3'2'0973—dc21

2002011495

Copies available from:

Naval Studies Board
National Research Council
2101 Constitution Avenue, N.W.
Washington, DC 20418

National Academy Press
2101 Constitution Ave., N.W.
Box 285
Washington, DC 20055
800-624-6242
202-334-3313 (in the Washington metropolitan area)

Copyright 2002 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

2

Nuclear and Radiological Threats

THE NUCLEAR AND RADIOLOGICAL THREAT MATRIX

For the purposes of the following discussion, the threats to homeland security from nuclear and radiological terrorism are grouped into the following three categories:

1. *Stolen state-owned nuclear weapons or weapons components*, modified as necessary to permit terrorist use.
2. *Improvised nuclear devices* (INDs) fabricated from stolen or diverted special nuclear material (SNM)[1]—plutonium and, especially, highly enriched uranium (HEU).[2]
3. Attacks on *nuclear reactors* or *spent nuclear fuel* or attacks involving *radiological devices*.

The threat matrix is summarized in Table 2.1 and is discussed in more detail below.

State-Owned Nuclear Weapons or Weapons Components

Several countries possess nuclear weapons that could potentially be turned to terrorist use: Britain, China, France, India, Israel, Pakistan, Russia, and the United States. Other countries have had weapons development programs in the past, and

[1]Special nuclear material includes fissile isotopes such as uranium-233, uranium-235, and plutonium-239 that can be used to make nuclear weapons.

[2]HEU contains ≥20 percent by weight of uranium-235.

000978

one of these (South Africa's) led to the development of nuclear weapons. Iran, Iraq, and North Korea are believed to have active weapons development programs at present, and these countries probably have the technical capabilities to develop nuclear weapons but may not have sufficient quantities of SNM (plutonium or HEU).

The weapons arsenals of Britain, China, France, Israel, and the United States are probably well protected. Indian and Pakistani nuclear weapons are also thought to be adequately protected at present, but the near-term (1- to 5-year) security of Pakistani weapons may be problematical. Theft or diversion of Russian nuclear weapons for terrorist use may represent a significant near-term threat to the United States, especially the theft or diversion of smaller, man-portable weapons. Table 2.1 and the classified annex provide additional details on these threats.[3]

Improvised Nuclear Devices

Improvised nuclear devices are nuclear weapons fabricated by terrorists, with or without state assistance, using stolen or diverted SNM. The basic technical information needed to construct a workable nuclear device is readily available in the open literature. The primary impediment that prevents countries or technically competent terrorist groups from developing nuclear weapons is the availability of SNM, especially HEU.

HEU could potentially be obtained by terrorists from several sources. There are large stockpiles of excess HEU and weapons-grade plutonium in both the United States and Russia, and other countries with nuclear weapons may have smaller stockpiles of these materials. HEU also exists in nuclear fuel from naval reactors, and large stocks of reactor-grade plutonium are contained in commercial spent fuel. Spent-fuel reprocessing programs and separated stocks of reactor-grade plutonium also exist in several countries, and these stocks are routinely transported across national borders. Reactor-grade plutonium can be used to fabricate workable nuclear devices.

Theft or diversion of excess Russian HEU for terrorist use represents a significant near-term threat to the United States. There are estimated to be about 150 metric tons of separated plutonium and 1,200 metric tons of HEU in Russia. The United States has been working with Russia over the past 7 years to secure this material and has made major progress. These safeguards are effective against casual thefts but may not be effective against higher-level threats, especially sophisticated insider threats. Moreover, a complete inventory of Russian materials is not available, so it is impossible to confirm that diversions of materials have

[3]In addition to the unclassified discussion of nuclear and radiological terrorism provided in this chapter, a classified annex containing further treatment of these topics has been produced by the study.

not already occurred. Additionally, there have been more than a dozen seizures of SNM from Russia and surrounding countries since the early 1990s. Most of the seized materials are thought to have been smuggled from Russian civilian nuclear sites.

Stocks of SNM also could be produced clandestinely, either through enrichment of uranium or reprocessing of spent nuclear fuel to recover plutonium. Uranium enrichment is equipment intensive and time consuming, and detection is increasingly likely as the scale of operations is increased. A small-scale program could potentially be hidden through careful facility design, however, and could, in principle, produce sufficient material for a weapon if operated for several years. Reprocessing to recover plutonium also can be carried out in small, difficult-to-detect facilities but requires access to irradiated reactor fuel. Any country with a research reactor has potential access to such fuel, and there are, in addition, large stocks of spent fuel in power reactors in countries of the former Soviet Union and also in foreign research reactors, some of which still operate with HEU. Clandestine production of SNM by states or terrorist groups for use against the United States represents a significant near-term threat to homeland security.

Nuclear Reactors, Spent Nuclear Fuel, or Radiological Dispersion Devices

The threats considered here include attacks on nuclear power plants (both commercial nuclear power plants (NPPs) and research reactors), their spent fuel storage facilities, and spent fuel transportation casks; detonation of conventional explosive devices packed with radioactive materials, so-called "dirty bombs;" and the surreptitious placement of radiation sources in places frequented by large numbers of the public. Attacks on DOE-owned nuclear facilities were not considered because these are generally considered to be hardened and well protected.

Nuclear Power Plants

The United States has 103 operating civilian nuclear power reactors at 65 sites that generate about 20 percent of the U.S. electrical supply (USNRC, 2002; EIA, 2002). The U.S. Nuclear Regulatory Commission (USNRC) regulates NPPs and has had a long-standing concern about security and safeguards. The agency's security and safeguards regulations are extensive and actively enforced.

The USNRC requires that NPPs be protected against a "design basis threat," defined at present to involve a ground attack by a group consisting of several armed terrorists aided by an inside collaborator.[4] NPPs are required to train their

[4]Additionally, some NPPs located near airports have been designed to withstand certain types of low-speed takeoff and landing accidents involving aircraft in common use when the plants were licensed in the 1970s.

TABLE 2.1 The Nuclear and Radiological Threat Matrix

TABLE 2.1A State-Owned Nuclear Weapons

Threat Category	Threat Description	Threat Level	Potential Consequences	Probabi of Occu
State-owned nuclear weapons	Theft and diversion of state-owned nuclear weapons for use, with or without modification, against U.S. targets or assets	United States: Low—weapons are well protected and tactical weapons have integrated permissive action links to prevent unauthorized use Britain, China, France, Israel: Low—weapons are few in number relative to U.S.-Russian arsenals and are well protected Pakistan, India: Medium—weapons are under secure control of the military, but political situation is unstable Russia: Medium—large numbers of weapons with poor inventory controls	Potentially catastrophic—massive loss of life and severe political and economic destruction possible	Modera 5 years. potentia

security personnel against this threat and are periodically tested by the USNRC to ensure readiness to meet this threat.

The current design basis threat for NPPs does not include high-speed attacks with fully loaded civilian airliners or, alternatively, smaller general aviation aircraft loaded with high explosives (HE) or attacks from the ground using HE projectiles. Potential targets for aircraft or ground attacks against an NPP are described in the classified annex.

The USNRC is supporting work at the Sandia National Laboratories, and the nuclear industry's trade association, the Nuclear Energy Institute (NEI), is directing work at the Electric Power Research Institute (EPRI) to assess some of these threats. These studies, which involve modeling aircraft impacts against steel-reinforced concrete structures and investigating the potential effects of aircraft-fuel fires, are proceeding independently of each other and will not be completed until after this report is published.

The details of these studies are classified and/or sensitive, and the results are

:es	Probability of Occurrence	Technical and Policy Challenges	Approaches to Mitigation
:— :s of life political iic possible	Moderate over the next 5 years, with a high potential for surprise	Theft or diversion may not require state assistance and may go undetected if theft occurs in Russia Stolen or diverted weapons could be converted for terrorist use HEU-based weapons smuggled into the United States could be difficult to detect and recover First responders may be killed or incapacitated by attack	Improve indications and warnings capabilities Improve security of Russian and Pakistani nuclear weapons at storage sites and borders Accelerate deployment of sensor arrays at critical U.S. entry points and targets Develop and announce policies to deter use of weapons by terrorist states Improve attribution capabilities

preliminary. But taken together, these studies suggest that a terrorist attack on an NPP could have potentially severe consequences if the attack were large enough. The severity is highly dependent on the specific design configuration of the NPP, including details such as the location of specific safety equipment. Additional details are provided in the classified annex.

The potential vulnerabilities of NPPs to terrorist attack seem to have captured the imagination of the public and the media, perhaps because of a perception that a successful attack could harm large populations and have severe economic and environmental consequences. There are, however, many other types of large industrial facilities that are potentially vulnerable to attack, for example, petroleum refineries, chemical plants, and oil and liquefied natural gas supertankers. These facilities do not have the robust construction and security features characteristic of NPPs, and many are located near highly populated urban areas. The committee has not performed a detailed examination of the vulnerabilities of these other types of industrial facilities and does not know how they compare to

TABLE 2.1B Improvised Nuclear Devices

Threat Category	Threat Description	Threat Level	Potential Consequences	Probabi of Occ
Improvised nuclear devices	Theft or diversion of SNM for fabrication of nuclear devices for use against U.S.targets or assets	United States: Low—SNM is well protected Britain, China, France, India, Israel, Pakistan: Low—small amounts of materials are well protected Russia: High—large inventories of SNM are stored at many sites that apparently lack inventory controls ,and indigenous threats have increased	Potentially catastrophic—massive loss of life and severe political and economic destruction possible	Moder 5 years potenti

the vulnerabilities of NPPs. It is not clear whether the vulnerabilities of NPPs constitute a higher risk to society than the vulnerabilities of other industrial facilities.

Research Reactors

Research reactors are used primarily to produce neutrons and gamma rays for research and development, and they provide a testbed for education on reactor physics and operations. As of April 2002 there were 36 operating research reactors in 23 states, an additional 12 reactors were being decommissioned, and 7 had licenses only to possess radioactive material.[5] Most research reactors are

[5]Much of the factual information used in this section is taken from the USNRC Web site. See, particularly, <http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/research-reactors.html>, last accessed May 20, 2002.

ces	Probability of Occurrence	Technical and Policy Challenges	Approaches to Mitigation
c— ss of life political nic possible	Moderate over the next 5 years, with a high potential for surprise	Theft or diversion may not require state assistance and may go undetected Crude HEU weapons could be fabricated without state assistance HEU-based INDs smuggled into the United States could be difficult to detect and recover First responders may be killed or incapacitated by attack	Improve indications and warnings capabilities Consolidate SNM at Russian sites, improve inventory controls, and improve security at sites and borders Accelerate blend-down of Russian HEU Accelerate the development and deployment of SNM sensor arrays at critical U.S. entry points and targets Improve capabilities for remote detection of HEU Develop and announce policies to deter use of INDs by terrorist- states Improve attribution capabilities

located at universities or government laboratories,[6] and many university research reactors operate on a restricted basis and therefore do not generate much radioactive material.

With thermal outputs ranging from about 0.1 to 20 megawatts, U.S. research reactors produce much less radiation, heat, and waste (e.g., spent fuel) than do power reactors, whose thermal output is commonly 2,000-3,000 megawatts. Research reactors also generally have fail-safe shutdown systems, and most do not generate sufficient heat to be vulnerable to core accidents, even in the event of a coolant loss. The potential consequences of terrorist attacks therefore appear to be small relative to power reactors.

[6]In addition, the Department of Energy and the U.S. Army operate research and test reactors at several of their sites. The thermal output of these reactors ranges from 5 to 400 megawatts. These reactors are not licensed by the USNRC and are not considered in this discussion.

TABLE 2.1C Radiological Attacks

Threat Category	Threat Description	Threat Level	Potential Consequences	Probabil of Occu
Nuclear power plants (NPPs)	Ground or air assaults on civilian NPPs	High—Over 100 potential targets exist in the United States	Variable, ranging from reactor shutdowns to core meltdowns with very large releases of radioactivity	Potentia attacks i near terr
Research reactors	Ground or air assaults	High—there are 36 operating reactors	Little or no release of radioactivity likely	Unclear
Spent nuclear fuel in wet or dry storage	Ground or air assaults on spent fuel pools or dry storage casks	High—Potential targets exist at all commercial NPP sites	Little or no release of radioactivity likely	Potential attacks is next 5 ye would be locate or damage
Radiological sources	Attacks with dirty bombs or placement of radioactive sources in public places	Very high—radiation sources are numerous and highly dispersed worldwide	Few deaths likely, but potential for economic disruption and panic is high	High—ma means are available, few preve in place
Radioactive waste	Same as for radiological sources	Very high—radioactive waste is abundant worldwide and not well protected	Trivial—most types of radioactive waste potentially available to terrorists have low specific activity	High—ma means are available. few preve in place

Spent Nuclear Fuel in Wet or Dry Storage

All civilian NPPs contain storage facilities for spent nuclear fuel and, with few exceptions, all of the spent fuel produced by those reactors is being stored at the sites where it was produced. Approximately 42,000 metric tons of spent fuel are currently stored under water in large spent fuel storage pools for cooling and shielding purposes. These pools are constructed of steel-reinforced concrete and are typically located adjacent to reactor containment buildings.

At some NPP sites spent nuclear fuel also is being stored outside the power-plant buildings in dry casks on concrete pads. At present, about 3,000 metric tons of spent fuel are being stored in this fashion. The casks are constructed of one or more layers of stainless steel and steel-reinforced concrete. The spent fuel is stored in the casks in an inert atmosphere at low pressure. A consortium of

es	Probability of Occurrence	Technical and Policy Challenges	Approaches to Mitigation
nging r o core with very es of	Potential for 9/11-type attacks is high in the near term	Stopping airplane attacks that deliver large amounts of energy directly on target	Perform vulnerability analysis of NPPs Harden vulnerable NPPs and improve redundancies of critical safety systems
release of likely	Unclear in the near term	Providing security against all types of attacks	Minimize the amount of fuel stored onsite
release of likely	Potential for 9/11-type attacks is high over the next 5 years, but targets would be difficult to locate or severely damage	Stopping airplane attacks that deliver large amounts of energy directly on target	Perform vulnerability analysis of spent nuclear fuel storage sites Move vulnerable spent fuel in wet storage to dry cask storage
ikely, for ruption nigh	High—materials and means are readily available, and there are few preventive measures in place	Training first responders to deal with these types of attacks	Improve first responder capabilities Improve public education
t types waste ailable ave ictivity	High—materials and means are readily available, and there are few preventive measures in place	Training first responders to deal with these types of attacks	Improve first responder capabilities Improve public education

nuclear utility companies has applied to the USNRC for a license to construct a centralized dry-cask storage facility (the Private Fuel Storage Facility) in Utah west of Salt Lake City. This facility, if licensed and constructed, could house up to 40,000 metric tons of spent fuel contained in up to 4,000 above-ground storage casks on thick reinforced-concrete pads (Private Fuel Storage, 2002).

The threat of terrorist attacks on spent fuel storage facilities, like reactors, is highly dependent on design characteristics. Moreover, spent fuel generates orders of magnitude less heat than an operating reactor, so that emergency cooling of the fuel in the case of attack could probably be accomplished using low-tech measures that could be implemented without significant exposure of workers to radiation. Dry cask storage systems are very robust and would probably stand up to aircraft attacks as well.

Like dry storage casks, spent fuel transport containers are very robust and appear to offer similar protection against terrorist attack. Studies on the vulnerability of spent fuel transport containers to sabotage suggest that relatively little or no radioactivity would be released in the event of a terrorist attack, and the USNRC is now undertaking a package performance study that will examine fuel performance and source terms under a variety of impact situations. That agency is conducting a top-to-bottom review of potential vulnerabilities, including transport vulnerabilities, in the wake of September 11. In the meantime, it has issued advisories to its licensees to take additional precautions until these reviews are completed.

Radiation Sources and Radioactive Waste

A wide variety of radiation sources are used in the civilian economy for, among other things, industrial radiography, radiation therapy, university research, and natural resource exploration. The approximately 2 million sources licensed by the USNRC range in activity from millicuries to tens of kilocuries and typically contain penetrating gamma emitters like cesium-137, cobalt-60, and iridium-192; alpha emitters like radium-226 and americium-241; and beta emitters like strontium-90. Devices in which such sources are dispersed by explosives or other means are called radiological dispersion devices (RDDs).

In the United States, most radioactive sources are regulated by the USNRC or by states under agreement with that agency, and a materials license is required to possess such sources. Licensees are responsible for safeguarding these sources and returning them to the manufacturer or properly disposing of them when the sources are no longer needed. This system is not foolproof, however. For example, according to USNRC records, several hundred U.S. sources are unaccounted for and presumed lost.

Radioactive sources are also used widely in other countries, not all of which have the regulatory controls that exist in the United States. Control of sources may be a particular concern in some central and eastern European countries, which lack strong regulatory or accounting standards.[7]

The United States also produces quantities of radioactive waste that could potentially be used in an RDD. This waste includes high-level spent nuclear fuel and high-level defense waste stored at government or commercial sites; transuranic waste stored at government sites; and low-level industrial, research, and medical waste stored at commercial sites, universities, and hospitals. Low-level waste may be a particularly attractive terrorist target: It is produced by many companies, universities, and hospitals, it is not always stored or shipped under tight security, and it is routinely shipped across the country. Although labeled

[7]See Gonzalez (1999) for a recent review of lost and stolen radioactive sources.

"low-level," some of this waste has high levels of radioactivity and could potentially be used to make an effective terrorism device.

RDD attacks could be carried out in several ways. Nonexplosive sources could be hidden in facilities frequented by large numbers of the public (e.g., sports stadiums, subway systems) or dispersed in building ventilation systems. Additionally, a radiation source could be combined with an explosive to disperse radioactive contamination over areas on the order of hundreds of square meters to a few square kilometers, depending on meteorological conditions. A radioactive waste shipment also could be attacked while in transit. Although such an attack probably would not disperse large quantities of radioactivity, it could cause public panic, especially if the attack took place in a highly populated urban area.

Detailed studies of RDDs suggest that few if any human deaths would be expected from dispersed radiation, although the explosion itself could cause casualties. The presence of dispersed radioactivity in the attacked area could, however, confound rescue efforts. The most severe effects on human health are produced if the material can be efficiently dispersed in respirable form. For optimum particulate sizes, inhaled material can remain lodged in the lungs, leading to either acute or chronic effects, depending on the amount and type of material respired. Although there are methods to construct an RDD to obtain good dispersion of inhalable particles, they require expert knowledge and access to university-level laboratory facilities.

HOMELAND SECURITY CHALLENGES

The threat matrix presented in Table 2.1 and discussed in previous sections suggests that the United States faces several near-term (1-5 year) vulnerabilities to terrorist acts using nuclear and radiological dispersal weapons. Several potential vulnerabilities are described in this section.

State-Owned Nuclear Weapons and Improvised Nuclear Devices

At present, the United States has no evidence that a terrorist organization or nonnuclear state possesses stolen nuclear weapons or INDs. However, this situation could change rapidly over the near term if steps are not taken to better secure nuclear weapons and SNM, especially in Russia. In the future, efforts to develop INDs may involve virtual collaborations among groups of countries and terrorist organizations. These efforts will be harder to detect and interdict because the different materials, facilities, activities, and expertise will be spread across large and unconnected geographical areas. As noted above, the primary impediment to the success of IND development efforts is the availability of SNM, especially HEU. The first challenge, then, for the United States and its allies is to improve security for weapons and special nuclear material wherever they exist, but especially in Russia.

Once a terrorist state or organization is able to procure a state-owned nuclear weapon or SNM, especially HEU, it will be able to fabricate an IND if it has the appropriate technical expertise. In addition to the potential for obtaining SNM from existing stocks in countries like Russia, the technologies for making SNM are ubiquitous, and past experiences, which are discussed in the classified annex, illustrate the difficulty of detecting well-concealed clandestine efforts to produce these materials. Therefore, the second challenge for the United States and its allies is to improve the gathering of indications-and-warnings intelligence on efforts by states or groups to obtain a nuclear capability so that resources can be focused on countering the most significant threats. The third challenge is to improve capabilities for detecting and interdicting stolen nuclear weapons and INDs once they are obtained by a terrorist group or state.

The consequences of terrorist use of a stolen weapon or IND are horrible to contemplate. A successful detonation of a stolen weapon or IND could produce massive casualties and cause substantial damage to the nation's political and economic infrastructure. Although recovery would eventually occur, it would be both expensive and lengthy. While recovery plans should be put into place to deal with such attacks, the main focus of the nation's efforts must be on prevention of attacks by whatever means possible.

Nuclear Reactors, Spent Nuclear Fuel, and Radiological Dispersion Devices

Nuclear power plants may present a tempting high-visibility target for terrorist attack, and the potential for a September 11-type surprise attack in the near term using U.S. assets such as airplanes appears to be high. Such attacks could potentially have severe consequences if the attack were large enough and, were such an attack successfully carried out, could do great harm to the nation's near-term energy security and civilian nuclear power as a long-term energy option.

Complete denial of the means to attack NPPs from the air or ground using U.S. assets such as aircraft is probably not feasible. If important vulnerabilities are identified, however, design and operational fixes exist, some of which are easily identifiable, that could substantially harden the facilities. Some of these possible fixes are discussed in the classified annex.

The private ownership and operation of NPPs present some additional challenges. One involves cost, and another information sharing. Private companies may be hesitant to commit significant resources to reducing vulnerabilities unless they receive clear guidance and leadership from the USNRC. Further, operators may be unable to pass such costs on to consumers in a highly competitive electricity market. This has important ramifications for nuclear energy as a long-term contributor to the U.S. energy supply. Information sharing between government agencies and plant owners and operators on potential vulnerabilities and operational fixes is essential for improving security at the nation's NPPs. Such infor-

mation sharing is currently problematical, however, because much of the information to be shared is classified.

Of course, the development of remedies for reducing potential NPP vulnerabilities to terrorist attack must consider both *costs* and *achieved risk reductions*, especially in view of the potential vulnerabilities of other types of industrial facilities, as discussed elsewhere in this chapter. The nation's resources to address these vulnerabilities are limited and thus have to be expended in a way that achieves the greatest risk reduction at the lowest overall cost to society.

Given the wide use of radiation sources in the United States and other countries, a determined terrorist would probably have little trouble obtaining material for use in an RDD. Fortunately, many radiation sources are strong gamma emitters and, unless heavily shielded, can be readily detected with existing sensor technologies. If an RDD attack were to occur, the casualty rate would likely be low, and contamination could be detected and removed from the environment, although such cleanup would probably be expensive and time consuming.

It is clear that the aim of an RDD attack would be to spread fear and panic and to cause as much disruption to society as possible. Given the public fear of anything "nuclear" or "radioactive," even a minor terrorist attack could have greatly magnified psychological and economic consequences. The ease of recovery from an RDD attack would depend to a great extent on how the attack was handled by first responders, political leaders, and the news media, all of which would help to shape public opinion and reactions.

REDUCING VULNERABILITIES

Several steps can be taken over the near term to reduce the nation's vulnerability to acts of nuclear and radiological terror. Science and technology have an important role to play in this effort but clearly are insufficient in themselves to meet the future challenges. Policy and procedural changes may also be required, as described in the following discussion.

Stolen Nuclear Weapons and Improvised Nuclear Devices

There are no obvious technological silver bullets to reduce the nation's vulnerability to terrorist use of stolen nuclear weapons or INDs. Nevertheless, science and technology can play a central role in an *enduring, multilayered homeland-defense system* that provides for the following capabilities:

- Indications and warnings of terrorist group membership, structure, intentions, and transformational activities;
- Accounting of and security for weapons and SNM inventories at their sources;

- Detection and interdiction, using technology and intelligence, of weapons and SNM moved across national borders, especially Russian and U.S. borders;
- Detection of weapon or IND movements inside the United States;
- Effective responses to nuclear and radiological attacks if they do occur; and
- Attribution to identify weapons and/or SNM characteristics and sources of origin.

Such a system must be structured to overcome the political inertia that inevitably develops over time and that can lead to a slackening of effort. A good example of such inertia is the federal government's reduced willingness to provide funding during the last decade to the Federal Aviation Administration (FAA) for air marshals to guard commercial flights against hijackers. It appears that the FAA's effectiveness in reducing airline hijackings through the 1980s led to a perception that the risk of hijacking no longer existed.

Protection, Control, and Accounting of Nuclear Weapons and Special Nuclear Material

Nuclear weapons and SNM can be most effectively protected, controlled, and accounted for at their sources, which are relatively few in number compared with the many potential points of transit across national borders and are protected by state-run security infrastructures. Therefore, the first line of homeland defense against nuclear and radiological terrorism is a robust system for protecting, controlling, and accounting for nuclear weapons and SNM at their sources.

Technology for weapons and SNM protection, control, and accounting already exists and has been deployed in many nuclear countries. The impediments to more widespread deployment of these technologies in nuclear weapons and SNM states include cultural differences over what constitutes workable and acceptable technologies; funding for procurement, training, and security screening of the necessary personnel; and the willingness of states to accept and deploy such systems.

Of particular concern is the deployment of these systems in Russia, which possesses large stockpiles of weapons and SNM, and Pakistan, whose weapons are controlled in a fashion that may be unpredictable, especially given the potentially unstable governmental situation. The United States can—and should—engage nuclear weapons states, states possessing SNM, and the International Atomic Energy Agency (IAEA) in bilateral and multilateral discussions aimed at improving the protection, control of, and accounting for weapons and SNM. To this end, the following four actions should be taken:

Recommendation 2.1: The U.S. government, working through the Department of Energy, Department of Defense, and Department of State, should

increase the urgency and pace of discussions with states possessing nuclear weapons and special nuclear material with the goal of identifying and implementing more effective safeguards through the wider deployment of protection, control, and accounting technologies.

Although the United States has technically sophisticated capabilities to offer to other nations, other nations have also identified good technical solutions to many of these challenges. Technology sharing is essential for preventing the unauthorized procurement and use of nuclear weapons.

Recommendation 2.2: Concurrently, the U.S. government, working through the Department of Energy and Department of Defense, should reexamine the security of its own nuclear weapons, both within its borders and elsewhere.

Stolen U.S. nuclear weapons represent a very small threat in the universe of threats described in this chapter; nevertheless, protecting these weapons is solely the responsibility of the U.S. government, and a reexamination to determine their security would set a positive example for other nuclear powers to emulate. In particular, the risks and benefits of retaining forward-based nuclear weapons in NATO countries should be reassessed, especially in light of the 2001 Nuclear Posture Review, which emphasizes that the addition of non-nuclear strike forces to the U.S. deterrent capability will reduce U.S. dependence on nuclear forces.[8] Although the presence of forward-based nuclear weapons in NATO countries does not pose an immediate danger given current levels of security and protection measures, the potential for rapid, regional changes in the geopolitical security environment is cause for concern.

Recommendation 2.3: The U.S. government, working through the Department of Energy and Department of Defense, should undertake an internal evaluation of its bilateral Materials Protection, Control, and Accounting (MPC&A) program in Russia and consider ways to accelerate progress in safeguarding nuclear weapons and special nuclear materials, especially to counter potential insider threats. A principal goal of this evaluation should be to identify ways to accelerate deployments of means to safeguard (1) atomic demolition munitions and other small nuclear warheads and (2) special nuclear material, particularly highly enriched uranium.

This program is moving at an irregular and sometimes interrupted rate for a variety of reasons, but there are several actions the United States could take to

[8]Transmittal letter of the 2001 Nuclear Posture Review to Congress, signed by Donald H. Rumsfeld. The classified review was completed in December 2001. There are other technical and diplomatic issues relevant to the nuclear posture that would have to be considered in this reassessment, including binding agreements with NATO countries.

improve its reach and effectiveness. These include (1) encouraging more of the work under this program to take place through direct scientist-to-scientist contacts; this may help to promote a better understanding of workable approaches for both countries and (2) reconceptualizing the program as a fully joint program of technology research, development, and deployment[9] that can serve to improve Russian security and raise worldwide safeguard norms.

The first essential step in a robust MPC&A program is an accurate estimate of SNM inventories, which appears to be lacking in Russia. To address this problem, the United States should work with the Russian government to obtain an accurate inventory of its weapons-usable materials to match the U.S. declaration (DOE, 1994, 1996, 1998) in a way that addresses Russian national security concerns.[10]

Recommendation 2.4: The U.S. government, working through the Department of Energy, should increase the priority and pace of cooperative efforts with Russia to safeguard its highly enriched uranium by blending down this material as soon as possible.

One way to accomplish this objective is to encourage Russia to down-blend HEU in two stages: the first to just less than 20 weight percent to eliminate the proliferation threat, and the second to those levels (typically 4 to 5 percent) required for sale as feed for reactor fuel. This two-stage approach would not require any more time or effort than the one-stage process used at present,[11] and the first stage probably could be accomplished in about 2 years if adequate funding were made available.

Recommendation 2.5: The U.S. government, working through the Department of State, Department of Energy, and U.S. Nuclear Regulatory Commission, should provide encouragement as well as technical and financial assistance to the International Atomic Energy Agency to raise the levels of

[9]This effort could involve scientists and engineers from both countries, and one of its explicit goals could be to improve protection, control, and accounting technologies and practices and to share these improvements with other countries and organizations, especially the International Atomic Energy Agency.

[10]For example, the Russian government could make a secret declaration, certify to the United States that such a declaration had been made, and provide the declared inventories to the U.S. government in encrypted form as evidence of this certification. The Russian government would hold the encryption key and might, at some time in the future, make that key public so that the inventory could be verified.

[11]The same uranium hexafluoride (UF_6) gas flow would blend four times as much uranium-235 to 20 weight percent as to 4.4 percent, and the down-blending facility in Russia could handle at least twice the current gas flow. Furthermore, accelerating the pace of down-blending would not disrupt world uranium markets, because the availability of 4.4 percent uranium-235 for nuclear fuel is limited by its rate of sale by Russia to world markets and not by the rate of down-blending. Accelerating the pace of down-blending may require international cooperation beyond that of the United States.

international norms for protecting civilian special nuclear materials, specifically highly enriched uranium from research reactors and civilian plutonium from intact and reprocessed spent nuclear fuel.

The assistance could include technical support and funding for safeguards-technology development and deployment activities. The United States also should encourage other nuclear states to provide support for this effort.

Detection and Interdiction of Illicit Weapons and Special Nuclear Material

An important line of defense in a layered system of homeland protection is the detection and interdiction of illicit nuclear weapons and SNM as well as the detection and disruption of illicit weapons development programs. Science and technology can contribute to this defense effort in at least two ways: (1) by providing technical means for detecting the movement of SNM, especially HEU, either in weapons or as contraband, through border transit points and around critical U.S. assets such as ports, cities, and other high-value facilities; and (2) by providing sophisticated data-mining tools for analysis of intelligence on nuclear smuggling and on illicit weapons development programs.

The presence of certain types of penetrating radiation is a signature of most (but not all) SNM. Passive detection of gamma rays and/or neutrons can be an effective screening technique in some circumstances for revealing the presence of illicit SNM or INDs. In other cases, active interrogation methods may be required. While shielding can reduce these signals, they can serve as a useful first indicator of SNM, as well as other radioactive materials that could pose threats.

The nuclear materials of primary interest in weapons and INDs are plutonium, primarily plutonium-239 and plutonium-240, and HEU. Plutonium can be detected through passive gamma-ray and neutron monitoring, but HEU is difficult to detect passively owing to its low specific activity, low spontaneous fission rate, and low-energy gamma-ray emissions. Passive monitoring of these materials requires large-area detectors and relatively long exposure durations for acceptable sensitivity. HEU can be detected by active monitoring using, for example, neutron detectors and pulsed neutron sources. Additionally, both HEU and plutonium can be detected indirectly by gamma radiography, which is sensitive to high-atomic-number materials. Active systems are more complex and costly than passive detectors, however, and they emit radiation. Consequently, there may be radiological safety issues associated with their use in populated areas.

The full deployment of a national detection network would be an expensive proposition given the large numbers of international transit points, entry points into the United States, and critical U.S. cities and facilities. Although sensor technologies now exist for such deployments, it will be a daunting technical challenge to integrate these technologies into effective and reliable detection systems—in particular, to sort through the thousands of hits that would be re-

ceived each hour from legitimate transport of commercial radioisotopes (including isotopes implanted or injected into people for medical tests and treatments), identify and track suspicious targets while the threats they pose are being evaluated, and dispatch responders to interdict the target if the threat proves credible, all in real time. A poorly designed system would likely be turned off or ignored by frustrated operators and responders once the false alarms reached even moderate levels. The state of the art for such detection systems has not yet advanced to the levels needed to make a national deployment feasible.

A careful analysis of likely SNM transport routes, however, would likely reveal a smaller number of choke points where well-designed detection systems could be effectively deployed. Such choke points might include the following:

- Critical border transit points in countries like Russia;
- Major global cargo-container ports, especially at cargo entry and transfer portals;
- Major U.S. airports with large numbers of international arrivals;
- Major choke points in the U.S. interstate highway system—for example, through the Rocky Mountains; and
- Major roadways, bridges, and tunnels into critical U.S. cities.

The deployment of sensor systems even at a large number of such choke points would not guarantee the detection of SNM in transit—determined terrorists probably could find ways to overcome such systems by using secondary entry points and roads or by using heavy shielding. But the deployment of a well-tested, national integrated detection network would be a powerful component of the layered homeland defense system.

A national detection network could consist of several types of sensors: large numbers of simple counters that indicate the presence of radiation, backed up by smaller numbers of spectroscopic instruments to identify specific isotopic signatures. The technical challenge for the deployment of both types of sensors is the differentiation of signals of interest from the background of naturally occurring radioactivity and medical and industrial radioisotopes. There is a surprising lack of comprehensive data on the normal variations in background and radioactivity in general commerce.

Small hand-held ("pager") radiation detectors are becoming available to customs officials, police, and first responders. These instruments could form the first layer of detection defense for illicit radioisotopes (especially strong gamma emitters) and could also be used by emergency personnel when responding to suspected radiological incidents. At present, most of these instruments have no spectroscopic discrimination capabilities; additional R&D would be needed to develop low-cost instruments of this type with spectroscopic capability and to improve their sensitivity and selectivity. Fixed instruments at airports or other

choke points can provide very useful sensitivity for materials in luggage or carried in truck cargo. R&D to support the innovative design and production of cost-effective detectors to meet these needs could be an important path to progress.

The following actions should be taken to improve the nation's capabilities to detect the illicit movement of weapons and SNM:

Recommendation 2.6: A focused and coordinated near-term effort should be made by the Department of Energy, through its National Nuclear Security Administration, and by the Department of Defense, through its Defense Threat Reduction Agency, to evaluate and improve the efficacy of special nuclear material detection systems that could be deployed at strategic choke points for homeland defense.

The objectives of these evaluations should be to provide (1) technical feedback to system developers that can be used to improve system design and performance; (2) improved definition of background signals at potential monitoring sites and radioisotopes in general commerce that can be used to improve system capabilities to detect illicit materials in transport; and (3) experience in detecting materials in transport that can be used to develop protocols for identifying false positives and evaluating and responding to actual threats.

Recommendation 2.7: Research and development support should be provided by the Department of Energy and Department of Defense for improving the technological capabilities of special nuclear material detection systems, especially for detecting highly enriched uranium.

In the near term. R&D is needed to improve neutron interrogation sources (i.e., neutron generators) and detector systems for HEU. Additionally, some priority should be given to the development of inexpensive portable detectors with spectroscopic discrimination capabilities so that such detector systems could be more widely deployed.

As mentioned above in this chapter, future efforts to develop INDs may be harder to detect and disrupt because such efforts are likely to involve multiple organizations spread across the globe. Detection of such efforts will require the ability to assemble intelligence data from many disparate sources and to find patterns and connectivity among large amounts of seemingly unrelated data. This will require the development of new databases, for example, databases that can be used to track and attribute smuggling efforts; enhancements to the connectivity of various kinds of databases (e.g., intelligence, immigration, law enforcement, signals intelligence, and imagery) to enable searching for relevant data; and the development of sophisticated data-mining tools and techniques that can identify transnational patterns and connections in the acquisition of know-how, technology, and materials for fabricating illicit weapons.

000990

Effective Responses to Nuclear and Radiological Attacks

Responses to nuclear and radiological attacks fall into two distinct categories that could require very different types of governmental actions: (1) attacks involving the detonation of a nuclear weapon or IND and (2) attacks involving RDDs. The first type of attack would likely involve massive property destruction and loss of life, making it difficult to mount an effective emergency response, at least over the short term. An emergency response action lasting months to years might be required in the wake of such an attack. The second type of attack would likely involve localized loss of life and no immediate danger to surrounding populations or property, but the potential for misinformation and public panic would be high. An emergency response action lasting weeks to months might be required, although longer-term cleanup might be needed for large RDD attacks. The worst scenarios involving nuclear power plants fall somewhere between these two categories, but, as noted in the classified annex, studies have not yet determined how credible these scenarios are.

Responses to nuclear and radiological attacks are governed by the Federal Radiological Emergency Response Plan,[12] which establishes authorities and procedures for responding to "peacetime" radiological emergencies such as accidents at nuclear power plants. This plan devotes only three paragraphs to radiological sabotage and terrorism, giving the Federal Bureau of Investigation the lead for investigating such acts and calling on other agencies, especially the designated lead federal agency, to assist the bureau in its investigative mission. The plan concludes that acts of sabotage and terrorism should not be treated as separate types of emergencies but are simply a "complicating dimension" of the other types of emergencies.

The correctness of this conclusion seems questionable given the attacks that might be envisaged in light of September 11. A terrorist attack could be much larger in magnitude than other events anticipated under this emergency plan. Such an attack could require large numbers of rescuers and medical personnel trained to deal with radiological emergencies; the ability to manage large populations in contaminated urban areas for long periods of time, potentially years; the ability to predict in real time the spread of radioactive contamination in debris clouds and provide this information to potentially affected populations in real time so that appropriate actions can be taken; and timely and effective cleanup capabilities. The current plan does not appear to provide the guidance needed to ensure this type of response in the case of nuclear terrorist attack.

---

[12] *Federal Radiological Emergency Response Plan—Operational Plan*, published by the Federal Emergency Management Agency in the *Federal Register* on May 1, 1996, with a correction published on June 5, 1996. The plan is available online at <http://www.au.af.mil/au/awc/awcgate/frerp/frerp.htm>. Accessed on April 22, 2002.

Recommendation 2.8: Immediate steps should be taken by the Federal Emergency Management Agency to update the Federal Radiological Emergency Response Plan, or to develop a separate plan, to respond to nuclear and radiological terrorist attacks, especially an attack with a nuclear weapon on a U.S. city. This plan should, at a minimum, address the following needs: (1) rapid mobilization of nationwide medical resources to cope with burns, physical trauma, and poorly characterized outcomes of exposure to radiation; (2) rapid airlift of field hospitals to the affected area; (3) means to provide the affected public with basic information on protection against radiation and fallout; (4) technical procedures for decontaminating people, land, and buildings; and (5) protection of citizens and foreign nationals from vigilante attacks. This plan should be mock exercised and, if required, incident site monitoring capabilities should be enhanced. Steps also should be taken to ensure that federal decision makers are familiar with this plan.

Should a nuclear or radiological attack occur, response effectiveness could be enhanced through public education efforts carried out well in advance of a nuclear or radiological attack. These efforts could include the stocking of potassium iodide pills by individuals to reduce the potential for thyroid cancers from releases of radioactive iodine. Such efforts may increase the public's willingness to accept market-based recovery approaches for land use and permitted activities in regions that are contaminated at levels just a few times above background radiation levels.

Attribution to Identify Characteristics of Weapons and Special Nuclear Material and Their Sources of Origin

As the history of the Cold War has shown, the most effective defense against attacks with nuclear weapons is a policy of nuclear retaliation. This past success suggests that the United States may be able to deter some future state-supported or state-sponsored nuclear and radiological terrorist acts by announcing in advance that it will retaliate by whatever means deemed appropriate, including the use of nuclear weapons, against states and terrorist groups responsible for nuclear or radiological attacks against U.S. citizens or assets.[13] To be a useful deterrent, however, this doctrine would have to be formulated and announced in advance, and its credibility would depend in large part on the ability of the United States to demonstrate to the rest of the world that it has the technical means to attribute such attacks to states or terrorist groups.

[13]The analogy between the Cold War and post-September 11 worlds is imperfect in that terrorist activity is dispersed geographically and may not be politically motivated. A doctrine of assured retaliation probably would not deter fanatical terrorist groups, but it may discourage states from providing such groups with aid and comfort.

000998

Attribution is a difficult technical challenge—ideally, one would want to know both the characteristics of the weapon used in the attack and its country of origin. The former can be determined through careful analysis of blast debris; the latter might be determined by linking this information with intelligence on thefts, smuggling, and weapons development efforts by states and terrorist groups developed through the data-mining techniques discussed above.

Efforts are under way by national laboratories to develop an attribution capability under the Defense Threat Reduction Agency (DTRA). The goal is to develop the capability to perform a postdetonation debris analysis and to draw conclusions on the design and performance after an attack. The technology for developing this capability exists but needs to be assembled, an effort that is expected to take several years.

Recommendation 2.9: Given the potential importance of attribution to deterring nuclear attacks, the Defense Threat Reduction Agency's efforts to develop a capability for identifying perpetrators of an attack should continue to declared operability as quickly as practical.

Reactors

The events of September 11 suggest that physical and operational changes at some NPPs may be needed to mitigate vulnerabilities to attacks from the air using a large commercial airliner or a smaller aircraft loaded with high explosives and, possibly, attacks from the ground using HE projectiles. The technical analyses that are now being carried out by the USNRC and EPRI to understand the effects of such attacks on reactor containment buildings and essential auxiliary facilities are critical to understanding the full magnitude of this threat to the nation's NPPs.

Recommendation 2.10: The ongoing U.S. Nuclear Regulatory Commission and Electric Power Research Institute assessments of nuclear power plant vulnerabilities to airliner attacks should be completed as soon as possible, and follow-on work to identify vulnerabilities on a plant-by-plant basis, including vulnerabilities to air attacks by small craft loaded with high explosives or to ground attacks by high-explosive projectiles, should be undertaken as soon as these initial studies are completed. This "completion" should not stand in the way of early actions to address significant plant vulnerabilities that are identified in the course of the ongoing Sandia National Laboratories and EPRI assessments. If these assessments continue to show that important vulnerabilities exist, then steps should be taken to reduce such vulnerabilities as soon as possible.

If the USNRC discovers significant vulnerabilities at its licensees' reactors as a result of these analyses, it could mandate a number of physical and opera-

tional changes to reduce vulnerabilities to and the consequences of attacks. Some possible changes are listed in the classified annex. This list is by no means exhaustive, and an effective remedy can be applied at a particular reactor only after a careful analysis of risks and benefits, taking into account the comparative risk reduction that could be achieved by devoting resources to hardening nuclear plants versus other large industrial facilities.

Radiological Dispersion Devices

Although the damage potential of RDDs is far less than that of stolen nuclear weapons, improvised nuclear explosives, or successful attacks on reactors, the terror/panic potential of RDDs warrants increased attention to the control and use of radiological sources by regulatory agencies and materials licensees.

Recommendation 2.11: The U.S. Nuclear Regulatory Commission and the states with agreements with that agency should tighten regulations for obtaining and possessing radiological sources that could be used in terrorist attacks (i.e., large sources containing long-lived isotopes), including requirements for securing and tracking these sources. Additionally, licensees possessing large sources should be encouraged to substitute nonradioactive sources (compact accelerators, electron beams, and x-ray generators) when economically feasible.

Other important counters to RDDs are public education, emergency responder training, and preparation of leaders to deal quickly and effectively with terrorist acts. As noted above, the likely aim of an RDD attack would be to spread fear and panic and cause disruption. Recovery would therefore depend on how such an attack is handled by first responders, political leaders, the media, and general members of the public.

In general, public fear of radiation and radioactive materials appears to be disproportionate to the actual hazards. Although hazardous at high doses, ionizing radiation is a weak carcinogen, and its effects on biological systems are better known than those of most, if not all, toxic chemicals. Federal standards that limit human exposure to environmental ionizing radiation, which are based on the linear, nonthreshold dose-response relationship,[14] are conservative and protec-

[14]That is, mutagenic (cell mutation) and carcinogenic (cancer) effects are assumed to increase linearly with radiation dose, with no threshold at low doses below which there is zero effect. A recent report by the National Council on Radiation Protection and Measurements concluded that "there is no conclusive evidence on which to reject the assumption of a linear-nonthreshold dose-response relationship for many of the risks attributable to low-level ionizing radiation . . ." (NCRP, 2001, p. 7).

tive, and the government continues to fund R&D[15] to improve scientific understanding of radiation effects on biological materials.

Education and training can serve as an effective counter to future RDD attacks. To this end, the committee recommends that the following actions be implemented:

Recommendation 2.12: Training should be provided to emergency responders (police, fire, and other emergency service personnel) on how to assess on-the-ground hazards from radiological attacks. As part of this training, responders should be provided with simple but effective radiation-monitoring devices, trained in their use, and told whom to contact for expert assistance, if needed. The Office of Homeland Security should take the lead for this effort in cooperation with the National Nuclear Security Administration and the Federal Emergency Management Agency.

Recommendation 2.13: Prepackaged kits of written materials on basic radiation science and effects should be developed for the media and national, state, and local leaders to help them respond appropriately to radiological attacks. The Office of Homeland Security should take the lead for this effort and should work with independent credible organizations to develop these kits.

Recommendation 2.14: A technically credible spokesperson at the national level who is perceived as being outside the political arena—for example, the President's Science Advisor, the Surgeon General, or their designated spokespersons—should be prepared to provide accurate and usable information to the media and public concerning public health and safety risks and appropriate response actions in the aftermath of a nuclear or radiological attack.

Such a response needs to be prepared and rehearsed in advance to avoid the kind of national leadership confusion that followed the anthrax attacks on Washington, D.C., in 2001.

[15]The Department of Energy sponsors research on low-dose radiation effects within the Office of Science and also supports the Radiation Effects Research Foundation, which is conducting a long-term longitudinal study of Japanese atomic bomb survivors. Additionally, the federal government provides funding to the National Research Council's Biological Effects of Ionizing Radiation (BEIR) Committees for periodic reassessments of low-dose health effects. The BEIR-VII study is currently in progress, and its objective is to determine the mathematical relationship between health risks and radiation dose for low levels of ionizing radiation.

CONCLUDING DISCUSSION

Many of the recommendations offered in this chapter call for an organized, focused, and adequately funded R&D effort to counter nuclear and radiological terrorism, as well as additional scientific, technical, and policy actions to reduce the nation's vulnerability to terrorist attacks, sometimes in cooperation with other national governments. To be effective, these efforts must bring to bear the best scientific and technical resources available to the federal government and must be well coordinated with other federal R&D and counterterrorism activities.

Important progress is already being made by the R&D and policy communities to reduce the nation's vulnerability to nuclear and radiological terrorism. There is not much evidence, however, that the R&D activities are being coordinated, that thought is being given to prioritizing these activities against other national counterterrorism needs, or that effective mechanisms are in place to transfer the results of these activities into application. Presumably the newly established Office of Homeland Security will take a lead role in the national counterterrorism effort, but that office does not have the expertise or budget to oversee a broad R&D effort.

The effectiveness of the nation's counterterrorism efforts could be improved if one agency were given the lead responsibility for coordinating and prioritizing, in consultation with other interested agencies, nuclear and radiological counterterrorism R&D. Several federal agencies have R&D responsibilities and could potentially take the lead: DOE's National Nuclear Security Administration (NNSA) already has a large R&D effort on many of the issues addressed in this chapter and is carrying out that work at the three national laboratories under its control.[16] The DOD's DTRA is carrying out R&D work to reduce threats from chemical, biological, and nuclear weapons of mass destruction. This work is being carried out primarily by DOD contractors, including NNSA national laboratories. The USNRC also sponsors R&D on NPP safety and vulnerabilities, and some of this work is carried out at NNSA national laboratories.

Given its large budget and broad scope of current work, it appears that DOE-NNSA is best positioned to take a lead role for R&D on nuclear and radiological terrorism. The committee, however, has not had an opportunity to study this issue in detail, especially to examine the current R&D portfolios of NNSA and DTRA or their strategic planning documents. The President's science advisor, working with DOE, DOD, USNRC, and other agencies with a stake in this decision, may be in the best position to develop a recommendation to the President regarding which agency should take a lead role in this important R&D effort. The designation of a lead agency also will require approval from the U.S. Congress.

[16]Lawrence Livermore National Laboratory, Los Alamos National Laboratory, and Sandia National Laboratories.

Recommendation 2.15: A single federal agency, possibly the Department of Energy's National Nuclear Security Administration, should be designated as the nation's lead research and development agency for nuclear and radiological counterterrorism. This agency should develop a focused and adequately funded research and development program to fulfill this mission and should work with other federal agencies, the President's science advisor, and the director of the Office of Homeland Security to coordinate this work and ensure that effective mechanisms are in place for the timely transfer of results to the homeland defense effort.

The centralization of lead R&D responsibilities into a single federal agency is no guarantee of success absent commitments to certain operating principles. Among these are commitments to appoint a technically capable staff to manage the R&D work; to provide sufficient and sustained funding to carry out an adequate program; and to reach across agency boundaries and outside government to obtain the expertise needed to execute the work and to ensure that results are moved expeditiously into application. While the events of September 11 appear to have produced a renewed sense of cooperation among federal agencies, the challenge for whichever agency is selected to lead this important R&D effort will be to nurture and sustain this spirit.

REFERENCES

Department of Energy. 1994. *Openness Press Conference Fact Sheets*, Office of the Press Secretary, Washington, D.C.

Department of Energy. 1996. *Plutonium: The First 50 Years*, Washington, D.C., 82 pp.

Department of Energy. 1998. *Commercial Nuclear Fuel from U.S. and Russian Surplus Defense Inventories: Materials, Policies, and Market Effects*, DOE/EIA-0619, Energy Information Administration, Washington, D.C., 115 pp.

Energy Information Administration. 2002. *U.S. Nuclear Generation of Electricity*. Available online at <http://www.eia.doe.gov/cneaf/nuclear/page/nuc_generation /gensum.html>.

Gonzalez, A.J. 1999. "Strengthening the Safety of Radiation Sources and the Security of Radioactive Materials: Timely Action," *IAEA Bulletin*, Vol. 41, No. 3, pp. 2-15.

National Council on Radiation Protection and Measurements. 2001. *Evaluation of the Linear-Nonthreshold Dose-Response Model for Ionizing Radiation*, Report No. 136. Bethesda, Md., 287 pp.

Private Fuel Storage. 2002. *The PFS Facility Specifications*. Available online at <http://privatefuelstorage.com/project/facility.html>.

U.S. Nuclear Regulatory Commission. 2002. *List of Power Reactor Units*. Available online at <http://www.nrc.gov/reactors/operating/list-power-reactor-units.html>.

AVIATION WEEK'S
www.AviationNow.com
Your Information Runway

Home | Sign In/Out | Site Map | Contact Us | About Us

PUBLICATIONS B2B COMMERCE CAREERS REFERENCES STORE

SEARCH
Advanced Sear

COMMERCIAL AVIATION
Top Stories | Calendar of Events | Forums | Classified & Careers | Photo Gallery

Choose Ch

HOMELAND SECURITY & DEFENSE
Homeland Security & Defense: Special Report

SEE ALSO:
America Confronted

PUBLICATIONS
AviationDaily
Click here for a free trial!

AVIATION WEEK
Browse The Latest issue's Contents

STOCK INFO

AVIATION WEEK
Airline 25

FEATURES
- Labor
- Airbus/Boeing
- FAA Benchmarks
- AMR, TWA
- UAL, US Airways

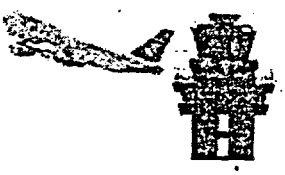
PROFILES (pdf)
- Major Airlines
- Regional Airlines
- Cargo Airlines

OUTLOOKS

Planes Often Enter Prohibited Air

AP

05-Apr-2002 2:41 PM U.S. EST



Despite military patrols and tighter security, pilots have intruded into America's protected airspace at least 567 times since Sept. 11, highlighting the continued challenges of thwarting a terrorist airstrike.

In each case, a pilot wrongly flew into one of the country's six prohibited flight zones, where no planes are allowed, or into one of many restricted zones where air traffic is limited because of sensitive military or nuclear operations or special events.

The post-Sept. 11 incidents include four commercial jetliners and one medical helicopter that flew into the forbidden airspace protecting the White House, Capitol and vice presidential mansion in the nation's capital, officials said. The most recent incursion occurred this week.

"Practically speaking, by the time a violation is discovered, it is too late to do anything to prevent a crash into the White House," former FAA security chief Billie H. Vincent said.

FAA Deputy Administrator Monte R. Belger said Thursday the agency recognizes there's little time to react once planes penetrate the safety zone and so the government has imposed numerous other precautions to ensure planes with ill intent don't get close.

"The restricted area is kind of the last line of

SEARCH SPECIFICATIONS TABLE

Commercial Aviation

ENTER SEARCH TERMS

Search

QUESTION OF THE DAY
What aircraft beat out the Martin six jet-engine XB-48 in a 1944 competition?
See Quiz & Answers

AEROPOLL
With Jane Garvey's five-year term as U.S. FAA administrator coming to an end in less than six months, how would you rate her performance?
Cast your vote

Button Advertiser Link

001004

- Freighters
- Commercial Transport
- Global Fleet/Capacity

Post-Show Wrap-Up

RELATED STORIES

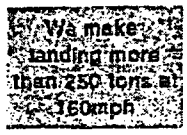
Mechanics Sue To Block Northwest's Background Checks

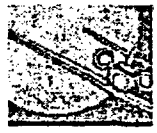
Mechanics Sue To Block Northwestâ€™s Background Checks

SAS Rejects Sweden's Proposal To Increase Immigration Checks

Cosmetic "Knife" Shuts Down Delta Hub at Cincinnati

defense," Beiger said. "The additional on-the-ground security procedures and in-flight protocols put in place give us a much higher level of confidence."





Borders have been tightened; pilots, flight crews and passengers are screened to weed out possible terrorists, and planes approaching Washington or other prohibited zones must complete authentication procedures, including providing passwords.

FAA enforcement records obtained by The Associated Press show most pilots who have violated protected airspace over the past decade usually walk away with nothing more than a warning letter.

Of the 111 pilots on 94 flights that flew into Washington's no-fly zone since 1992, just one was fined, for $1,000, and nine had their licenses suspended for between seven to 120 days, the records show. At least 90 were settled with administrative action -- nearly all of them warning letters, the analysis showed.

Just a month before the September hijackings, a Mesa Airlines flight strayed into prohibited airspace over Washington. By November, the matter was closed with a warning letter to the pilot -- common for most cases.

Between Sept. 11 and March 5, the FAA recorded 567 airspace violations across the country, ranging from prohibited airspace to special use zones where only certain planes may fly.

Of that number, 65 involved incursions into major prohibited or restricted sites. Nineteen of those cases already have been resolved with no punishment or administrative letters, officials said.

Former Transportation Department Inspector General Mary Schiavo, who highlighted airline safety problems in the 1990s and now works as a lawyer representing airline accident victims, said the small number of severe punishments amounts to laissez-faire enforcement.

"It is fairly typical. The FAA really doesn't like to do enforcement actions, particularly any carrier infringement," said Schiavo, a frequent FAA critic.

FAA officials said they had no plans to stiffen the penalties, unless the number of incursions keeps growing. They said in most cases pilots mistakenly intruded the airspace or were blown into it by high winds.

001005

"They generally aren't deliberate. They generally don't reflect poor skills or poor training," Belger said. "If we do see a situation that is egregious or reflects a lack of training ... we take appropriate action."

Planes that violate Washington's prohibited zone are quickly warned by air traffic controllers to correct course, and the Secret Service is alerted. Nearly all pilots comply immediately, officials said.

Military planes that patrol the capital skies are permitted to force such planes to land or, as a last resort, shoot them down if pilots don't respond.

None of the five planes that flew into the capital's protected space since Sept. 11 have required such action, officials said.

Washington's Reagan National airport was closed for more than a month after the attacks, and has been gradually reopened to traffic since despite reservations by the Secret Service.

One pilot died when he crashed his small plane into the White House in September 1994; no one else was harmed. In 1999, a pilot drifted so close to the White House that agents fired a warning flare. That pilot ended up with a warning letter, FAA records show.

The five most recent airspace violations are still being investigated, including a Frontier Airlines 737 jet that flew over the White House and vice presidential residence on Monday before correcting its path. That pilot has been grounded with pay pending the outcome of the investigation.

FAA records show violators of Washington's airspace over the past decade include about three dozen pilots for major commercial airlines, one Air Force pilot, a NASA pilot, a handful of private or foreign pilots and several air transport companies.

One pilot caught in Washington's prohibited airspace blamed air traffic controllers, saying they are so busy they sometimes order flight maneuvers that send pilots into the prohibited zone.

"The D.C. controllers are absolutely horrible. Washington National is absolutely the worst place to fly into, period," said Happy Wells, a 30-year veteran pilot from Oklahoma who was cited in July 1997 for flying his charter plane through Washington's prohibited zone.

001006

Wells said his proposed penalty was rescinded

after he filed a report with the FAA.

Outside Washington, there are five other prohibited zones: President Bush's ranch in Crawford, Texas; the Bush family compound in Kennebunkport, Maine; the presidential retreat at Camp David in Thurmont, Md.; the Pantex nuclear assembly plant in Amarillo, Texas; and the area around George Washington's home at Mount Vernon, Va.

Elsewhere, there are numerous permanent and temporary restricted zones across the country. They cover military and nuclear sites, special events like the Winter Olympics in Utah and the Super Bowl in New Orleans, or places like New York and Boston where threats have prompted temporary zones

Since many restricted areas are temporary, FAA notifies pilots through a monthly publication. Over the past month, for example, the agency has warned pilots to stay out of certain areas such as a zone surrounding an auto race in Talladega, Ala., areas hosting aerial demonstrations by the Navy Blue Knights and Air Force Thunderbirds; and parts of Alaska where the officials are setting off pre-emptive avalanches.

The McGraw-Hill Companies

Copyright 2002 ©AviationNow.com All Rights Reserved.
Terms under which this service is provided to you.
Read your privacy guidelines.

001007

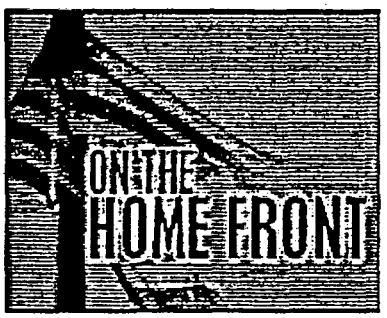
it saves time

hpi ProLiant BL e-Class roll over for specs

NETZERO PLATINUM
SIGN UP NOW!

abcNEWS ON DEMAND

ABC NEWS.com ShoppingGuide



Subways, Scuba Divers, and Landmarks

Also: House Approves $29 Billion Anti-Terror Bill; Terrorist Chief's Interrogation Leads to More Threat Warnings

Terrorists May Use Scuba Divers, Planes

WASHINGTON, May 24 — Terrorists may use scuba divers or small planes to attack targets in the United States, the FBI said today in the latest in a series of unconfirmed warnings.

"Recent information has determined that various terrorist elements have sought to develop an offensive scuba diver capability," the FBI said in an information bulletin issued by its National Infrastructure Protection Center.

"While there is no evidence of operational planning to utilize scuba divers to carry out attacks within the United States, there is a body of information showing the desire to obtain such capability," the FBI said.

Citing "uncorroborated information," the FBI also discussed possible terrorists using small planes.

"The interest is reportedly in the use of small aircraft, as opposed to large, commercial aircraft, due to post-September 11, 2001 enhancements in aviation security throughout the United States," the FBI and the Transportation Security Administration said in an alert to law enforcement.

The warnings are the latest in a string issued this week. Federal transportation officials said in an alert made public Thursday that they have gotten an unconfirmed warning that terrorists are planning attacks on subways in the United States.

The possible attack would involve simultaneous strikes against multiple trains, perhaps using time bombs, said an alert issued by the Department of Transportation's Office of Intelligence and Security and obtained by ABCNEWS.

Although the warning specified subways, it advised all mil

Although the warning specified subways, it advised all rail and transit security officials to review their safety procedures and "implement additional security measures commensurate with the current threat environment."

It emphasized that the threat was not confirmed, but advised the industry to remain on a heightened state of alert.

The subway warning is particularly unsettling to New Yorkers, where millions of people ride the city's subways every day. Residents there were told this week that the Brooklyn Bridge or the Statue of Liberty could be targeted by terrorists.

And around the country, federal officials warned building managers to be on the lookout for terrorists trying to rent apartments for the purpose of planting explosives. Apartment building management companies sent copies of the warning to residents of some buildings in New York and Los Angeles earlier this week.

— *ABCNEWS.com*

House Approves $29 Billion Anti-Terror Bill

WASHINGTON, May 24 — The House approved $29 billion early today for the fight against terrorism overseas and at home as the two parties grappled in a bitter election-year spat over war and the growing national debt.

Democrats and Republicans alike strongly backed the money the package would provide. Billions would be showered on the military, on Afghanistan and other U.S. allies, on rebuilding New York, and on the Coast Guard, explosive detection devices for airports, and other anti-terror initiatives.

Even so, the measure's 280-138 passage came only after bleary-eyed lawmakers had battled until nearly 3 a.m. ET over issues that could resound in this fall's campaigns for congressional control. The overnight session highlighted a GOP resolve to not start lawmakers' Memorial Day recess without passage of a counterterrorism bill they could tell voters about.

Over three days of unusually acerbic debate, Democrats accused Republicans of sneaking a borrowing increase into the bill while the GOP said Democrats were hindering money sorely needed by American troops abroad.

"They retreated from our responsibility to put politics aside when the time comes to strengthen our country," taunted House Majority Whip Tom DeLay, R-Texas.

That prompted Democrats to accuse Republicans of smearing them by questioning their patriotism, as all pretenses that the war against terror should not become a political issue seemed to fade away.

"We don't want those soldiers used for your agenda," said Rep. Patrick Kennedy, D-R.I.

The Senate's anti-terror legislation was facing its own contentious path. The appropriations committee passed a $31 billion version of the bill on Wednesday. But Republicans, eager to trim it closer to the $27.1 billion President Bush proposed in March, blocked debate until Congress returns next month.

More than half the House's Democrats ended up voting against the bill. Their chief objection was that majority Republicans had forced language into it that would pave the way for raising the current $5.95 trillion cap on federal borrowing.

The Bush administration wants a $750 billion boost in that limit enacted by late June, saying an unprecedented federal default otherwise awaits. It will be the first since 1997, when annual deficits turned to surpluses under President Clinton.

Democrats concede a borrowing increase is inevitable, but say it was forced by last year's GOP-written tax cut. They say that means Social Security surpluses will have to

be diverted to pay for other programs — which while true will not affect the program's benefits or solvency, but gives them a political issue to raise.

The money is for the remaining months of fiscal 2002, which ends Oct. 1. It is the second installment of anti-terrorism spending since the Sept. 11 attacks, following $40 billion lawmakers approved late last year.

The military would get the lion's share of the money: $14 billion in the Bush and Senate proposals, $15.8 billion under the Senate bill. Those funds would go for everything from bomb guidance systems to the Reserves and National Guard.

New York would get $5.5 billion under all three plans to rebuild from the Sept. 11 attacks on lower Manhattan. Most of the rest is for domestic security programs like staffing the new Transportation Security Administration, modernizing FBI computers and buttressing security at Energy Department nuclear weapons facilities.

The House bill would temporarily freeze the $10 billion loan guarantee program that Congress created late last year to help airlines whose business was eroded by the terrorist strikes.

US Airways officials have lobbied unsuccessfully so far to remove the provision, which lawmakers supporting them said could mean the airline will go out of business this summer. GOP leaders say the carrier should be able to get loans to carry it over until the fall, when the federal loans will be available again.

The Senate bill trims the loan program to $429 million this fiscal year and to $4 billion permanently.

— *The Associated Press*

Terrorist Chief's Interrogation Leads to More Threat Warnings

WASHINGTON, May 24 — The words of Abu Zubaydah have set counterterrorism officials into motion again, even as they wonder if the captured al Qaeda field commander is lying just to create panic.

Law enforcement and other U.S. officials, speaking on condition of anonymity, said Thursday that Abu Zubaydah's claims led to this week's warnings of potential terrorist attacks on the Brooklyn Bridge and the Statue of Liberty.

He did not provide a date or method of attack, and officials called his statements uncorroborated. But they canceled a 119th birthday celebration for the bridge anyway.

The level of the U.S. response to the warnings is a testament to Abu Zubaydah's seniority within al Qaeda, officials say. He is the highest-ranking terrorist leader to come into U.S. custody since the Sept. 11 attacks on the World Trade Center and Pentagon. Officials have been able to verify at least some of his statements to CIA and FBI interrogators.

"He has told us things we didn't know before that we subsequently were able to confirm," said one senior official. "Not everything he says is bogus."

On the other hand, officials say some of his statements are certainly lies or boasting, intended to promote al Qaeda's ends by confusing investigators and scaring Americans. Abu Zubaydah speaks English.

Other threats from Abu Zubaydah have reached the public's ears: He was the key source for last month's threat to banks in the northeastern United States, and he also claimed al Qaeda was building a radiological weapon, a so-called dirty bomb that spreads harmful radioactive substances but does not ignite a nuclear detonation.

Officials have said threats linked to Abu Zubaydah are only publicized when they match other information.

He also recently told his interrogators that United Airlines Flight 93, the hijacked plane that crashed in Pennsylvania on Sept. 11 after its passengers fought back, was aimed at the White House. Officials had previously assumed the White House was its likely destination but said the U.S. Capitol and CIA headquarters were other potential targets.

Intelligence officials say al Qaeda typically keeps going after the same target until it conducts a successful strike, noting the 1993 attack on the World Trade Center as well as the January 2000 attempt to bomb a U.S. destroyer in Yemen — months before the successful bombing of the USS Cole.

Officials describe Abu Zubaydah, a Saudi-born Palestinian, as a link between bin Laden and many of al Qaeda's operational cells. Abu Zubaydah ran the Khalden camp in Afghanistan, where U.S. investigators believe many of the Sept. 11 hijackers trained.

He also had telephone contacts with at least one student at U.S. flight schools, according to a July 10, 2001, memo from a Phoenix FBI agent.

Earlier, he is believed to have masterminded the failed millennium bombing plots in Los Angeles and Jordan, and he has been linked to failed plots on the U.S. embassies in Paris and Sarajevo.

U.S. and Pakistani authorities captured and wounded Abu Zubaydah in a raid in Faisalabad, Pakistan, in late March.

They also found his notebook, which officials say may contain a more accurate account of his plans.

His location remains undisclosed but he is thought to be away from U.S. soil.

He shouldn't know the furor his statements are causing, if his interrogators are using standard techniques that would keep him uninformed. This would allow them to tell him only what they want about events in the outside world.

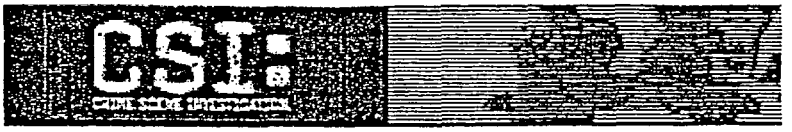
— *The Associated Press*

PRINT THIS PAGE | SEND THIS TO A FRIEND | VIEW MOST EMAILED

Copyright © 2002 ABCNEWS Internet Ventures.

Click here for: HELP ADVERTISER INFO CONTACT ABC TOOLS PR TERMS OF USE PRIVA

Family of sites: ABC.com ABC Family ESPN.com Disney.com FamilyFun.com GO M



Dozens Of Airport Workers Arrested

WASHINGTON, April 23, 2002

(CBS)

"There will be zero tolerance of security breaches at our nation's airports."
Attorney General John Ashcroft

(CBS) Federal authorities Tuesday rounded up 94 workers at Washington-area airports on a variety of charges from illegal immigration to lying about a criminal background, Attorney General John Ashcroft announced.

The arrests at Dulles and Reagan National airports were part of a continuing post-Sept. 11 crackdown by U.S. law enforcement and transportation authorities on airport security lapses.

Ashcroft said the workers allegedly gained access to secure areas of the airports "by lying on security applications," using false Social Security numbers or committing "various immigration frauds."

"There will be zero tolerance of security breaches at our nation's airports," Aschroft said.

CBS News Correspondent Stephanie Lambidakis reports most of those arrested are Hispanic and none are being charged with terrorism-related offenses.

Tuesday's operation was a joint effort that included the FBI, the Immigration and Naturalization Service, federal prosecutors and the Transportation Department's inspector general.

Similar arrests have occurred in recent weeks in Phoenix, Las Vegas, Salt Lake City and San Francisco. In all, about 400 workers have been arrested since Sept. 11, including those on Tuesday, officials said.

The investigation, called Operation Tarmac, had spread to 10 airports before Tuesday's arrests.

Many of those arrested Tuesday were illegal aliens and could be deported; others face prison terms or fines of up to $250,000, officials said.

Most of the workers arrested had security badges allowing them to get onto planes, ramps, runways and cargo areas, law enforcement officials said. They were employed by private companies, such as those that clean the airplanes or operate airport restaurants.

While law enforcement officials said none of those arrested have been linked to terrorism, some aviation experts said the workers were in a position to help smuggle bombs or weapons aboard aircraft.

U.S. authorities believe that the Sept. 11 hijackers carried knives and box

INTERACTIVE

Eye On Air Safety

ENTER

See how turbulence affects an airplane, test your flight survival knowledge and see how black boxes help crash investigators piece together what happened.

INTERACTIVE

America On Guard

ENTER

The terror attacks in the U.S. and air strikes on Afghanistan have forced the nation to toughen its national security. Find out what actions are being taken to protect our nation in the air, water and on land.

RELATED STORIES & LINKS

Story
Closing Airport Security Holes

Story
Airport Security Vs. Efficiency

Story
Back To School For Airport Security

Story
DC Airspace Violations Not Unusual

Story
$2B Price Tag For Airport Security

Story
Airport Security Gets An 'F'

Story
Air Security vs. Commerce

001012

cutters past security checkpoints and there was no evidence that the weapons were put on board by rogue employees, a law enforcement official said, speaking on condition of anonymity.

© MMII, CBS Worldwide Inc. All Rights Reserved. This material may not be published, broadcast, rewritten, or redistributed. The Associated Press and Reuters Limited contributed to this report.

MORE INSIDE THIS SECTION

- Former Klansman Guilty Of Murder
- Chandra Levy's Body Found
- White House Served Enron Subpoenas
- FBI Nixed Flight School Probe
- Canine Killing Grounds
- A 'Mystery Illness' No More
- Toxic Algae Killing West Coast Animals
- Navy Sub Catches Fire

Back To Top

• Help • Advertise • Feedback • Terms of Service • Privacy Statement
©MMII, CBS Worldwide Inc, All Rights Reserved.

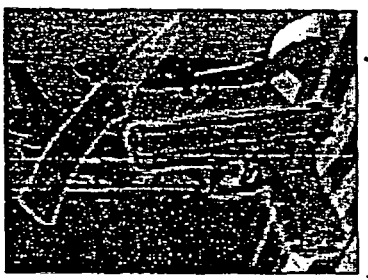
©cbsnews.com

©CBSNEWS.com

BIG BROTHER 3 Are you up for anything and everything?

Airport Security Gets An 'F'

March 25, 2002



(CBS/AP)

"The FAA and the TSA have worked closely with the inspector general's office to address security issues and have taken immediate action any time we've been notified about problems."
FAA spokeswoman Laura Brown

(CBS) The Transportation Department inspector general found airport security screeners on several dozen occasions failed to catch guns and simulated explosives, even after the September terrorist attacks, a person familiar with the report said Monday.

Inspector General Kenneth Mead's report found screeners missed knives 70 percent of the time, guns 30 percent of the time and simulated explosives 60 percent of the time, said the source, speaking on condition of anonymity.

CBS News Correspondent Jim Axelrod reports these findings support what a CBS News investigation first revealed last month. In that investigation, lead-lined film bags, which block x-ray exams, passed screenings unchecked 70% of the time.

Tests of the security system were conducted at 32 airports while the screening checkpoints were still primarily under the supervision of the airline industry, with some oversight by the Federal Aviation Administration. The new Transportation Security Administration took over responsibility for airline security Feb. 17.

Security administration spokesman Paul Turk said the White House requested the investigation. "The idea was to get a realistic assessment of potential needs," he said.

Some of the same companies doing the work during the audit period are still stationed at security checkpoints under contracts that will run until a new federal work force of screeners is phased in between May and mid-November.

Transportation Department officials would not comment on the audit details, saying its results were too sensitive to reveal publicly.

Aviation regulators defended actions to tighten security at airports in the months after Sept. 11.

"The FAA and the TSA have worked closely with the inspector general's office to address security issues and have taken immediate action any time we've been notified about problems," said FAA spokeswoman Laura Brown.

The security agency is hiring 30,000 federal employees to take over passenger screening. On Monday, it began training the first 300 of 1,200 senior supervisors, who will run the airport checkpoints. The other 900 will be

INTERACTIVE

America On Guard

ENTER

The terror attacks in the U.S. and air strikes on Afghanistan have forced the nation to toughen its national security. Find out what actions are being taken to protect our nation in the air, water and on land.

RELATED STORIES & LINKS

Story
Counterfeit Crackdown

Story
Phony IDs, Real Danger

Story
Airport Security Fails Test

Story
Nuke Plant Security Concerns

Story
Air Security vs. Commerce

Story
Security Switch At O'Hare

Story
New Airport Security Devices Debut

001014

trained over the next three weeks. The supervisors all have law enforcement, security or military backgrounds, Turk said.

Following several well-publicized post-Sept. 11 incidents, Transportation Secretary Norman Y. Mineta in October ordered government officials to close airport concourses and re-screen passengers.

Security breaches caused the government to evacuate 59 airport concourses or terminals between Oct. 30 and March 7, forcing 2,456 flights to be delayed or canceled, the FAA says. Passengers on another 734 flights had to leave their seats and go through security a second time, the FAA said.

Former FAA security chief Billie Vincent said the report was not surprising, considering the checkpoints were staffed by the same low-paid, poorly trained screeners who were there before Sept. 11.

In addition, Vincent said, current equipment cannot detect explosives, nor can it detect many varieties of cutting tools.

"The technology at the screening points is not there," Vincent said. "The current metal detectors won't do the job. If you turn it high enough to detect that much metal, you will have an alarm on every person going through."

©MMII CBS Worldwide Inc. All Rights Reserved. This material may not be published, broadcast, rewritten, or redistributed. The Associated Press and Reuters Limited contributed to this report.

More Headlines

- Pakistan Insists Border Is Secure
- Congressman: U.S. Plans Iraq Attack
- U.S. Warns Of Easter Threat In Italy
- Happy Homecoming For U.S. Sailors
- Judge: Let ACLU See Names
- Al-Aqsa Added To U.S. Terror List
- Aftershocks Jolt Afghanistan
- FBI: Terror Plot Against Israel Foiled

Back To Top

• Help • Advertise • Feedback • Terms of Service • Privacy Statement
©MMII, CBS Worldwide Inc, All Rights Reserved.

NUCLEAR CONTROL
INSTITUTE

THE IMPACT OF NUCLEAR PLANT SHUTDOWN ON SEVERE ACCIDENT CONSEQUENCES

Edwin S. Lyman, PhD
Scientific Director
DRAFT: February 12, 2002

OVERVIEW

In the core of an operating nuclear reactor, many different fission product isotopes are produced. Some have relatively long half-lives, such as cesium-137 (30 years). Others have relatively short half-lives. After the reactor is shut down, many of the short-lived fission products decay away rapidly, leading to a reduction in the "source term" --- e.g. the quantity of radionuclides that are available to be released in an accident. This memorandum presents the results of a calculation of the approximate reduction in consequences (both latent cancer fatalities and early fatalities from acute radiation syndrome) of a severe core melt accident following reactor shutdown.

LIMITATIONS

This calculation does not attempt to calculate any change in the probability of a core melt accident that may result from reactor shutdown. Numerous studies have indicated that the probability of core damage at nuclear plants during outages is comparable to the probability at full power. This result, however, may depend on the fact that much safety equipment is unavailable during outages for maintenance. The risk of containment failure from overpressure is likely to be lower at shutdown plants.

The calculation also assumes that the "release fractions" --- the fractions of core radionuclides that would be released to the environment in a severe accident --- are the same for both full-power and shutdown modes. This simplifying assumption is commonly made but does not take into account changes to the release fraction that may result from the different thermal and chemical conditions that the core would encounter during an accident in shutdown mode.

METHODOLOGY AND ASSUMPTIONS

A generic pressurized-water reactor (PWR) with a capacity of approximately 1000 MWe was analyzed. Core inventories were obtained using the Oak Ridge National Laboratory SCALE 4.3 code for an end-of-cycle (EOC) core at full-power and for a core at twenty days after shutdown. Code parameters were based on a typical U.S. PWR core management scenario. Additional details may be found in a recent publication.[1]

Severe accident consequences were calculated using the Sandia National Laboratories MACCS2 code. The calculations assumed uniform population densities of 354 persons/sq. km and 962 persons/sq. km for the regions within 10 miles of the plant and between 10 and 50 miles of the plant, respectively. These values correspond approximately to a total of nineteen million individuals within 50 miles, with 288,000 individuals within 10 miles --- the values for the Indian Point plant. A single set of weather conditions was chosen for simplicity. Finally, latent cancer fatalities calculated below do include chronic radiation exposures due to long-term contamination, but numerous generic assumptions were made for this estimate. None of these assumptions would be appropriate for an accurate, site-specific calculation of the absolute number of latent cancer fatalities in a particular region, since the results would depend strongly on the actual population distribution and weather conditions. However, they are adequate for the purposes of this calculation, which seeks to calculate the relative consequences of accidents during full-power and shutdown modes.

Appropriate release fractions for a severe accident with early containment failure were developed from U.S. Nuclear Regulatory Commission reports. Further details are available in Reference 1.

The calculations assume that 85% of individuals located within 10 miles of the reactor are evacuated. However, the relative consequence ratios obtained below are insensitive to this assumption.

RESULTS

Table 1 presents the results of the calculation.

	Full-power	20 days after shutdown	Ratio of SD to FP
Latent cancer fatalities within 50 miles	53,960	26,870	0.50
Acute fatalities within 10 miles	867	166	0.19

[1] Edwin S. Lyman, "Public Health Risks of Substituting Mixed-Oxide for Uranium Fuel in Pressurized-Water Reactors," *Science and Global Security* 9 (1) 33.

CONCLUSIONS

At twenty days after shutdown, a severe accident with containment failure will result in approximately 50% fewer latent cancer fatalities within 50 miles of the plant, and approximately 81% fewer acute fatalities within 10 miles of the plant, for the generic model considered.

SECURITY GAP: A Hard Look At the Soft Spots in Our Civilian Nuclear Reactor Security

Staff Summary of Responses by the
Nuclear Regulatory Commission
to Correspondence from
Rep. Edward J. Markey (D-MA)
Member, Energy and Commerce Committee
U.S. House of Representatives
March 25, 2002

EMBARGOED UNTIL MONDAY MARCH 25, 2002
12:01 AM

Contents

Heading	Page
Introduction	3
I) The NRC is Not Adequately Overseeing Security at Nuclear Reactors	4
A) The NRC does not know how many foreign nationals are employed at nuclear reactors, and does not require adequate background checks of nuclear reactor employees that would determine whether an employee was a member of a terrorist organization	4
B) The NRC does not know what its licensees spend on security or how many security guards are employed at each reactor	5
II) Nuclear Reactors and Impact by Aircraft	5
A) Twenty-one nuclear reactors are located within 5 miles of an airport	5
B) 96 percent of U.S. nuclear reactors were designed without regard to the potential for impact from even a small aircraft	6
C) Aircraft impact to the containment structure of a nuclear reactor is not the only way an aircraft could cause a full-scale core meltdown	7
D) The NRC has rejected placing anti-aircraft capabilities at nuclear facilities, even though other countries have chosen to do so and even though many reactors are located very close to airports	8
III) Security of Spent Nuclear Fuel is Inadequate	8
A) Spent nuclear fuel in significant quantities exists at reactors all across the U.S. and is stored in buildings that are not hardened structures	8
B) Security of spent nuclear fuel at decommissioned reactors is lower than that at operating reactors in part because licensees obtained exemptions to the security regulations. The NRC assumed that spent fuel fires would only occur as a result of an accident, and failed to consider fires that occurred as a result of a terrorist attack	9
C) The NRC has not experimentally determined how long a fire spent fuel casks can withstand, and has not provided information on worst-case consequences of a breach of a spent fuel cask	10
IV) Security at Nuclear Reactors Continues to be Inadequate Even After September 11th	10
A) It took the NRC almost 6 months after September 11th to require enhanced security at nuclear reactors	10
B) The NRC has historically failed to adjust the security regulations to meet the evolving threat, and has yet to begin a permanent revision of security regulations following the events of September 11	11
C) Security exercises at nuclear reactor sites are inadequate, and sites continue to fail the exercises about 50% of the time	12
Appendix A	14
Appendix B	17

Introduction

Following the terrorist attacks on the World Trade Center Towers and the Pentagon on September 11, 2001, Rep. Markey initiated a series of letters to the Nuclear Regulatory Commission regarding our nation's preparedness for similar attacks on civilian nuclear targets. The possibility of a terrorist attack on a civilian nuclear power plant is not new. In fact it is anticipated in requirements, referred to as the "Design Basis Threat," that all plant operators must meet when they build a civilian nuclear power-plant in the United States. Unfortunately, prior to 9-11, the NRC was in the process of systematically backing away from rigorous enforcement of those requirements, and post 9-11, it has failed to upgrade the Design Basis Threat to take into account the new reality of terrorists acting in large groups carrying a sophisticated understanding of the technical aspects of their target and a commitment to suicide as the price to be paid for accomplishing their goal. The threat is no longer theoretical. President Bush has remarked on the discovery of Al Qaeda documents showing the plans of civilian nuclear targets, and Al Qaeda operatives have given testimony asserting their interest in targeting nuclear materials and civilian nuclear power-plants[1].

Although Rep. Markey's concerns regarding the terrorist threat to civilian nuclear power-plants have been expressed in correspondence with the NRC over many years,[2] the basis of the current analysis can be found in the letters sent by Rep. Markey to the NRC following 9-11 (November 15, November 19 and November 27, 2001) and the NRC's responses forward to Rep. Markey on March 4, 2002 (hereafter referred to as the NRC Response). (The NRC has yet to respond to Rep. Markey's December 4, 2001 letter NRC regarding the security of radioactive materials.)

The NRC requested that some responses to these questions be kept confidential for security reasons. We have done so while compiling this analysis. The full correspondence (other than the documents NRC has requested we not make publicly available) on which this analysis is based can be found at http://www.house.gov/markey/iss_terrorism.htm.

---

[1] See, for example: "Bin Laden Sought Uranium, Jury Told," Washington Post, February 8, 2001; 2 Nuclear Experts Briefed Bin Laden, Pakistanis Say, Washington Post, December 12, 2001; President Bush State of the Union Address, January 29, 2002; "Nuclear Plants Targeted," Washington Times, January 31, 2002;

[2] See http://www.house.gov/markey/iss_terrorism.htm for copies of Rep. Markey's January 15, 1991, February 28, 1991 and January 27, 1992 letters to the NRC supporting a petition to require an upgrade to NRC's security rules for truck bombs and other threats, the May 8, 1997 letter to the NRC on combustibility of nuclear reactor materials, the November 8, 1998 letters to the National Security Counsel and the NRC on terrorism at nuclear reactors, the February 23, 1999 letter to the NRC on nuclear reactor terrorism, the July 8, 1999 letter to the NRC on the suspension of force-on-force security exercises, the February 4, 2000 letter to the NRC on radiological sabotage at domestic nuclear reactors, the September 20, 2001 letter to the NRC on nuclear reactor terrorism in light of the events of September 11th, the November 15, 2001 letter to the NRC on nuclear reactor terrorism in light of the events of September 11th, the November 19, 2001 letter to the NRC on security at spent nuclear fuel facilities, the November 27, 2001 letter on aircraft threats to nuclear reactors, the December 4, 2001 letter to the NRC on the security of nuclear materials and the January 16, 2002 letters to the NRC, U.S. Customs, Fedex and UPS on security associated with the shipment of radioactive materials.

The NRC Is Not Adequately Overseeing Security at Nuclear Reactors

Rep. Markey's letter requested information regarding the numbers and screening procedures for reactor employees who are foreign nationals, as well as information related to the security forces at each reactor. The responses indicate that the NRC is in the dark about what nuclear reactor licensees are doing to ensure the reactors are safe from attack.

A) The NRC does not know how many foreign nationals are employed at nuclear reactors, and does not require adequate background checks of nuclear reactor employees that would determine whether an employee was a member of a terrorist organization[3]

According to the NRC Response, NRC Personnel Access Authorization Requirements for Nuclear Power Plants requires that a *criminal* background check be performed on prospective employees seeking to obtain unescorted access to protected and vital areas of a nuclear power plant. However, the NRC Response states that "the search is limited to the United States" and that "Licensees determine access to the facility regarding foreign applicants on a "best effort" basis and the applicants are screened and processed as any other individual according to federal requirements." It is unacceptable that the NRC neither has a policy on screening of foreign nationals, nor does it know what its licensees' policies are. Terrorists may now be employed at nuclear reactors in the U.S. just as terrorists enrolled at flight schools in the U.S.

According to the NRC Response, crimes committed overseas by foreign job applicants are not even looked for. Moreover, although Rep. Markey requested whether *security* background checks would be conducted in order to determine whether an individual is a member of a domestic or foreign group that seeks to do harm to the U.S. (such as Al Qaeda), the NRC did not indicate that such checks have been performed in the past or would be done in the future. The NRC Response also stated that the NRC has no idea how many foreign nationals are employed at nuclear power plants, though individual licensees would have such records. It states that "the screening requirements do not require the [foreign] applicants to declare any affiliation with terrorist organizations, although the background investigation, including criminal history, may uncover information that may lead to discovery of such affiliation."

In short, it appears that Al Qaeda operatives such as Mohamed Atta or Marwan al-Shehhi could pass the narrow nature of the criminal screening still in use at U.S. nuclear power-plants and gain unescorted access to the controlled area of a plant, just as they obtained student visas to attend flight school. As long as they have no criminal record in this country, Al Qaeda operatives are not required to pass any security check intended to find and expose terrorist links prior to their employment.

[3] See Page 9-12 of the NRC Response

B) The NRC Does Not Know What Its Licensees Spend on Security or How Many Security Guards are Employed at Each Reactor

According to the NRC Response:

- The NRC has approved the use of new technologies that replaced security guards at some reactors. The NRC Response states that "the NRC does not require licensees to submit information concerning security expenditures. The NRC also does not have information on the number of security personnel at each facility over the last ten years."[4]

- The NRC Response states that "the number of security employees varies in accordance with a number of factors, including site design, geography, and response strategies."[5]

It is appalling that the NRC does not require licensees to submit information regarding the licensee's security resources, expenditures and capabilities. While new technologies may be a supplement to security guard forces, only security guard forces would be able to combat an armed attack on a nuclear reactor. The NRC must ensure that there are sufficient security guard forces to repel attacks by a large group of technologically sophisticated and suicidal attackers who may be assisted by insiders working at the reactors who disarm whatever new technologies have been installed.

II) Nuclear Reactors and Impact by Aircraft

A) Twenty-one nuclear reactors are located within 5 miles of an airport

Although an NRC Task Force recommended in NUREG-0625 that nuclear reactors not be sited within 5 miles of a major or commercial airport, the NRC acknowledged that 21 reactors are located within 5 miles of an airport[6]:

Name of reactor	Nearest city/town	Proximity to airport
Three Mile Island	Harrisburg, PA	3 miles from Harrisburg International Airport
Maine Yankee	Wiscasset, ME	1 mile from Wiscasset Municipal Airport
H. B. Robinson	Columbia, SC	2.2 miles from Hartsville Regional Airport
Limerick 1,2	Philadelphia, PA	2.2 miles away from Pottsdown-Limerick airport and 5 miles away from Pottsdown Municipal Airport
Seabrook	Portsmouth, NH	4.6 miles away from Hampton Airfield airport, 6.5 miles away from Cole Farm

[4] See Page 13 of the NRC Response
[5] See Page 14 of the NRC Response
[6] See Pages 83-84 of the NRC Response for airport information, and http://www.nrc.gov/reactors/operating/list-power-reactor-units.html for locations of reactors

		airport and 7.1 miles away from Plum Island airport
Wolf Creek	Burlington, KS	4.5 miles away from Coffey County airport
Clinton Power Station	Clinton, IL	located 4.5 and 4.75 miles away from 2 private airports
Catawba 1,2	Rock Hills, SC	4.2 miles away from Rock Hill airport
Dresden 2, 3	Morris, IL	Within 5 miles of 2 private airports
Brunswick 1,2	Southport, NC	4 miles away from Brunswick County airport
Palisades	South Haven, MI	located 3.6 miles away from South Haven Area Regional airport
Kewaunee	Greenbay, WI	3.7 miles from Ranch Side airport
Duane Arnold	Cedar Rapids, IA	4.6 and 5.3 miles away from 2 private airports
Braidwood 1,2	Joilet, IL	within 5 miles of 2 private airports
LaSalle 1,2	Ottawa, IL	located 2.5 and 4.3 miles away from 2 private airports

B) 96 percent (all but 4 of the 103) of U.S. nuclear reactors were designed without regard to the potential for impact from even a small aircraft.

The planes that struck the World Trade Center and the Pentagon were Boeing 757s and 767s which have a maximum takeoff weight of 272,500 - 450,000 pounds at takeoff. [7] What would happen if they had struck a U.S. nuclear reactor instead?

There are 103 active civilian nuclear reactors in the U.S. According to the NRC, the licensees of 43 of those reactors on 28 sites did not even consider the probability of an accidental aircraft impact when the reactors were designed, built and licensed. In an additional 56 reactors on 37 sites, the licensees concluded that the probability of an accidental aircraft impact was so low that it did not have to be incorporated into the designs for the reactors.

In no case has any U.S. licensee considered the possibility of a deliberate aircraft impact such as the one that occurred on September 11, 2001.[8]

According to the NRC Response, only 4 U.S. reactors include any design features calculated to withstand the impact of an airplane. The Limerick (Philadelphia, PA) and Seabrook (Portsmouth, NH) reactor designs were evaluated to consider impacts from aircraft weighing up to 12,500 pounds – less than 3-5 percent of the weight of the Boeing 757s/767s aimed at the World Trade Center and the Pentagon.[9]

Only the Three Mile Island units 1 and 2 near Harrisburg, PA, were designed with the impact of a large airliner in mind. According to the NRC Response, Unit 1 was

[7] See http://www.boeing.com/commercial/767family/technical.html and http://www.boeing.com/commercial/757-300/product.html
[8] See Pages 74-76 of the NRC Response
[9] See Page 73, 75 of the NRC Response

designed with "reinforcement of outer walls, thickening of concrete sections, and unique internal features. In addition, special fire protection and ventilation features were provided to cope with aircraft crashes. Similar features were incorporated in Three Mile Island Unit 2." The design features were made so that the reactors could withstand the impact of planes weighing up to 200,000 pounds.[10]

Nuclear reactors licensed by Switzerland are designed to withstand the impact of a 44,092 pound airplane traveling at 481 miles per hour, the reactor buildings have 1 meter-thick reinforced concrete walls, and spatial separation of redundant or diverse safety devices is required. According to the NRC Response, "Germany and possibly other European countries also require nuclear containment structures to withstand the crash of certain types of military and commercial aircraft."

The NRC Response states that the U.S. chose not to require additional protection against the impact of an aircraft because "The likelihood of an airplane accidentally crashing onto a reactor site in the U.S. is typically much lower than in Europe."[11]

C) Aircraft Impact To The Containment Structure Of A Nuclear Reactor Is Not The Only Way An Aircraft Could Cause A Full-Scale Core Meltdown

The NRC Response acknowledges that there are buildings other than the core of the reactor (which is a hardened structure) that could lead to a core meltdown if destroyed by the impact of a commercial aircraft:

- "The NRC recognizes that aircraft crashes may result in multiple-failure initiating events, and that non-safety system malfunctions could contribute to such events."[12]
- If all electrical power to a reactor was cut off (by a deliberate crash of an aircraft into the power generating systems, for example), the time it would take for damage to the reactor core to begin is estimated by the NRC to be about two hours[13].
- Support systems for the reactor, such as the cooling system, are not located within buildings that are hardened (such as the reactor core) and "are not designed to withstand the direct impact of a large commercial aircraft." The destruction of some of these buildings could lead to core damage.[14]

These acknowledgments by the NRC are highly significant, because they indicate that claims by the nuclear industry that existing plants would be able to withstand a terrorist aircraft or other attack due to the strength of containment structures are

[10] See Pages 71-72, 76-79, 83 of the NRC Response
[11] See Pages 32-33 of the NRC Response
[12] See Page 82 of the NRC Response
[13] See Pages 94-95, 97-99 of the NRC Response
[14] See Page 96 of the NRC Response

irrelevant to the very real risk that terrorists might target critical support infrastructure whose destruction could result in a catastrophic nuclear accident.

D) The NRC Has Rejected Placing Anti-Aircraft Capabilities At Nuclear Facilities, Even Though Other Countries Have Chosen To Do So And Even Though Many Reactors Are Located Very Close To Airports

The NRC Response states that it "believes that the proper way to deal with the potential hijacking of large commercial aircraft by suicidal terrorists is through the measures on airline security now well underway."[15] Temporary no-fly-zones above nuclear reactors were imposed on November 2, 2001 but were removed less than a week later. While it is our hope that airline security measures now well underway will prevent future hijackings, the absence of no-fly-zones and the proximity of many nuclear reactors to airports lead many experts to believe that anti-aircraft systems on the ground at or near reactor locations is necessary to assure security.

France has deployed anti-aircraft weaponry at its reprocessing facility in La Hague, and similar measures have reportedly been taken at nuclear facilities in Hungary.

Nevertheless, the NRC has concluded that it "sees no need to deploy anti-aircraft weaponry at any commercial nuclear facilities in the United States. After consultation with the Department of Defense, the Office of Homeland Security, and the Federal Aviation Administration (FAA), the Commission believes that there would be enormous command and control problems and a large potential for unintended consequences and collateral damages if such weaponry were deployed. The Commission believes that the proper way to deal with the potential hijacking of large commercial aircraft by suicidal terrorists is through the measures on airline security now well underway."[16]

The no-fly-zones around nuclear reactors were lifted after less than a week. The NRC has acknowledged that nuclear reactors were not designed to withstand the impact of a large commercial aircraft, and that 21 of the reactors in the U.S. are located within 5 miles of an airport. Rep. Markey strongly believes that equipping the reactor sites with anti-aircraft weaponry would enhance security greatly.

III) Security Of Spent Nuclear Fuel Is Inadequate

A) Spent Nuclear Fuel In Significant Quantities Exists At Reactors All Across The U.S. and Is Stored In Buildings That Are Not Hardened Structures.

Pages 38-41 of the NRC Response contain a 1998 table of how much spent nuclear fuel is stored in the spent fuel pool (i.e. outside the better-protected reactor core building) in each operating reactor in the country. The closest city/town to each reactor

[15] See Page 30 of the NRC Response
[16] See Page 30 of the NRC Response

was added by Rep. Markey's staff using information obtained from NRC's website.[17] The table is included as Appendix A of this report. At any reactor that has continued operating since the 1998 list was compiled, the amounts of spent nuclear fuel would, of course, have continued to accumulate and be higher today. Information on decommissioned reactors was not complete and does not seem to be available on the NRC website.

B) Security of Spent Nuclear Fuel at Decommissioned Reactors is Lower than that at Operating Reactors In Part Because Licensees Obtained Exemptions to the Security Regulations. The NRC Assumed That Spent Fuel Fires Would Only Occur As The Result Of An Accident, And Failed To Consider Fires That Occurred As A Result Of A Terrorist Attack.[18]

The NRC Response conceded that "NRC regulations do not require dry cask storage areas to be protected by armed guards or vehicle barriers" and that "A watchman is required with the ability to contact and have the local law enforcement agencies respond immediately to an event." The NRC also allowed licensees of these sites to reduce the amount of insurance coverage they must obtain. Force-on-force exercises have never been conducted at a decommissioned reactor in order to determine whether the exemptions to security requested and received by licensees were appropriate from a security perspective.

Prior to September 11th, the security requirements for non-operating reactors (i.e. those that contain stores of spent nuclear fuel but do not produce electricity any longer) were non-uniform because some licensees had obtained exemptions to the security regulations. Since September 11th, the NRC has issued a security advisory to require vehicle barriers and armed responders at these sites. However, as is noted on page 3 of the NRC Response, an advisory is a "guidance document that is not, in itself, legally binding."

The reason why licensees of these facilities requested and received exemptions from the security requirements is because the NRC assumed that the greatest safety risk at a decommissioned reactor, a zirconium fire, would only occur accidentally, and that the risk of such an accident was very low. NRC did not evaluate the risk that a terrorist attack could intentionally cause a zirconium fire, it did not attempt to update estimates for the costs associated with a zirconium fire, and failed to respond to Rep. Markey's questions related to whether it had performed worst-case analyses of the consequences of such a fire.

The NRC Response stated that "There is a possibility that, with enough explosives, both a spent nuclear fuel pool or spent fuel dry cask can be penetrated." However, in its consideration of whether licensees should be able to reduce safety and insurance coverage at these sites, the NRC assumed that a zirconium fire would be accidental and would therefore require more than 20 hours to ignite as a result of accidental

[17] See http://www.nrc.gov/reactors/operating/list-power-reactor-units.html
[18] See Pages 42-64 of the NRC Response for references for this section

drainage of the spent nuclear fuel pool. The NRC has not considered an "external heat source," such as an explosion caused by a terrorist attack, in arriving at the 20-hour estimate.

Rep. Markey strongly believes that all security exemptions received by licensees of these sites should be immediately revoked.Security at spent fuel sites needs to be dramatically and immediately upgraded and no lessening of this higher standard should be contemplated unless and until an economic, safety and health analysis of the worst-case consequences associated with a successful terrorist attack at these sites has been completed and has justified a reduction.

C) The NRC Has Not Experimentally Determined How Long A Fire Spent Fuel Casks Can Withstand, And Has Not Provided Information On Worst-Case Consequences Of A Breach Of A Spent Fuel Cask.

In prior correspondence, the NRC dismissed the possibility that a fire caused by an aircraft at a spent nuclear fuel facility would last for more than "a matter of minutes," because NRC assumed that only 200 gallons of jet fuel would be available to feed the fire. However, a typical large commercial aircraft contains more than 20,000 gallons of jet fuel.

The NRC Response states that "the staff performed an analysis of a seven-hour fire duration. The results from the analysis did not lead to fuel failure or cask failure."[19] The NRC does not cite a real-world *experiment* that demonstrated this seven-hour fire duration tolerance level for a spent-fuel cask, nor does it state the theoretical or experimental limit of how long a spent fuel cask can withstand a fire fed by jet fuel.

IV) Security at Nuclear Reactors Continues To Be Inadequate Even After September 11th

A) It Took The NRC Almost 6 Months After September 11 To Require Enhanced Security At Nuclear Reactors

On September 11th, the NRC issued a "Threat Advisory" that recommended security enhancements to its licensees. According to the NRC Response, a "Threat Advisory" is a "guidance document that is not, in itself, legally binding.[20]" The NRC issued an Order requiring security enhancements to its licensees on February 26, 2002, almost 6 months after September 11th. According to the NRC Response, "An order imposes legally binding requirements upon a licensee... If a licensee does not comply with the requirements of an order, civil penalties or additional sanctions for such noncompliance may be imposed by further order. Willful noncompliance with an order may result in criminal sanctions, pursuant to Section 223 of the Atomic Energy Act.[21]"

[19] See Page 35 of the NRC Response
[20] See Page 3 of the NRC Response
[21] See Page 3 of the NRC Response

It is unclear why, given the seriousness of the events of September 11th and the subsequent discovery of information about U.S. nuclear reactors in captured Al Qaeda locations that suggested they were potential terrorist targets, the NRC failed to impose legally binding security requirements on its licensees until February 26, 2002.

B) The NRC Has Historically Failed To Adjust The Security Regulations To Meet The Evolving Threat, And Has Yet To Begin A Permanent Revision Of Security Regulations Following The Events Of September 11th [22]

The Design Basis Threat (DBT) is the set of regulations that define the security threat against which all licensees must be protected. The DBT was first created in the late 1970s, and according to the NRC Response, was amended in minor ways in 1987 and 1994[23].

The DBT now in force, therefore, is based on assumptions of threat levels that date to the 1970s. These assumptions do not account for the realistic threat levels we now know to exist; the DBT assumes that only a small group of attackers would be involved, it assumes that a vehicle used for a truck bomb could only be as large as an SUV, it assumes only passive insider assistance from one insider at the reactor, and it fails to assume the degree of technical sophistication and modern weaponry that we know Al Qaeda members have access to.

The NRC has yet to even begin to permanently revise the DBT regulations to require licensees to protect against the realistic terrorist threat we know now exists, including but not limited to consideration of: attacks by more than "several" simultaneous attackers; attacks that involve the participation of more than one insider; attacks that involve the participation of an *active* insider(s) (i.e. one or more individuals who assist the attackers by opening locked doors or operating equipment during the attack); attacks using sophisticated weaponry such as vehicle-mounted weapons; and attacks by individuals possessing sophisticated knowledge of the operation of nuclear reactors such as the attackers who participated in the September 11th hijackings.

---

[22] See Page 6 of the NRC Response

[23] The first such change, in 1987, was to require licensees to consider that attackers might use a vehicle for use in transporting personnel and equipment during an attempted theft of strategic special nuclear material. It is unclear why the use of a vehicle was not anticipated as a possibility prior to 1987, since it seems obvious that anyone seeking to steal strategic special nuclear material would probably approach and leave the site in a car, truck, boat, or plane. The second such change, in 1994, was to a) require licensees to consider that attackers might use a vehicle for use in transporting personnel and equipment during an attempted act of radiological sabotage, and b) require licensees to consider that attackers might use a vehicle bomb as a means of attack. It is unclear why the use of a vehicle to transport personnel and equipment for use in sabotage was not considered in 1987, since it seems rather remarkable for the NRC to have concluded that attackers would use such a vehicle to steal strategic special nuclear material but not to commit an act of radiological sabotage. It must also be noted that the vehicle bomb regulation only requires licensees to protect against bombs contained in 4 wheel drive vehicles, even though much larger truck bombs have been detonated against U.S. targets both in the U.S. and abroad.

C) Security Exercises At Nuclear Reactor Sites Are Inadequate, And Sites Continue To Fail The Exercises About 50% Of The Time

The NRC has historically conducted force-on-force exercises, known as Operational Safeguards Response Evaluations (OSRE), to assess the adequacy of security at nuclear reactors In 1998, the NRC and the industry attempted to de-fund OSRE. After opposition from Rep. Markey and the public forced them to restore funding to the program, the NRC instead decided to replace the OSRE program with one that would be designed and run by the nuclear industry, called the Safeguards Performance Assessment (SPA). Rep. Markey believes that the proposed SPA program would undermine the rigor of current testing and has been proposed by the NRC and industry because they are simply embarrassed by the failure rate under OSRE and the accompanying revelation that security measures that look good on paper are not succeeding in the field.

Prior to September 11, the NRC intended to reduce the number of OSREs from eight to six each year, in order to undertake the SPA pilot program. The NRC Response to Rep. Markey's questions on security exercises at nuclear reactor sites indicates that:

- In 37 of 81 OSREs (46 percent of the security tests) conducted between August 1991 and August 2001, the NRC identified weaknesses that allowed the attacking force to "reach a target set and simulate destruction of that equipment... The licensee's performance is judged unsuccessful for the scenario if the response force is not able to prevent the adversary from disabling and/or destroying all pieces of equipment/actions in a target set.... Cases in which a licensee was unable to satisfy one or more of these criteria would indicate that the adversary could cause an act of sabotage resulting in a loss of a complete target set (i.e., the equipment necessary to be protected to prevent core damage)."[24]

- The NRC Response states that "for the 15 OSREs conducted between April 2000 and August 2001, weaknesses were identified in 9 of 59 exercises or 15 percent of the time.[25]" Compared to the 1991-2001 time frame, this appears at first to be a significant improvement. However, upon further examination of information contained in the non-public section of the NRC's response and discussion with the NRC staff, which agreed to the public disclosure of the statistical representation of this data, the NRC has conceded that if judged using the same method of analysis used for the August 1991-2001 time, **the NRC identified serious weaknesses at 7 of 15 OSRE sites, and required corrective action to be taken at 9 of 15 sites. In short, between August 1991 and August 2001, weaknesses were identified at 46% of the sites tested. Between April 2000 and August 2001, serious weaknesses were identified at 47% of the sites tested and corrective action was required at 60% of them.**

[24] See Pages 27-29 of the NRC Response
[25] See Page 27 of the NRC Response

- No force-on-force security exercises have been conducted since September 11 because "the current elevated threat environment would pose significant safety hazards to the licensees' employees and negatively impact security effectiveness."[26] Although licensees have advance notice of the date of the exercises, and the Department of Energy has resumed its force-on-force exercises at nuclear weapons facilities, the NRC has chosen to indefinitely postpone future OSREs. This means that the NRC has no way of knowing whether the enhanced security measures it ordered on February 26 actually succeed in enhancing security.

- The NRC intends to continue to move forward with the pilot program of the industry-designed and implemented SPA security program, instead of enhancing its own OSRE program. This will result in the reduced ability by NRC to participate in and oversee exercises designed to test security at nuclear reactors.[27] The NRC Response states that it "does not agreed that the testing of a licensee's security force needs to be the sole function of a federal entity, even in light of the September 11 events."[28]

[26] See Page 17 of the NRC Response
[27] See Pages 19-23 of the NRC Response
[28] See Page 24 of the NRC Response

APPENDIX A

SPENT FUEL POOL/FULL CORE OFFLOAD CAPABILITY - As of November 1998

(Number of fuel assemblies)

(Attachment to Answer 3.b)

CLOSEST CITY /TOWN	PLANT NAME	FUEL IN CORE	AVAILABLE SPENT FUEL POOL CAPACITY	FUEL IN SPENT FUEL POOL	REMAINING SPENT FUEL POOL CAPACITY
RUSSELLVILLE AR	Arkansas 1	177	968	818	150
	Arkansas 2	177	988	701	287
MCCANDLESS PA	Beaver Valley 1	157	1627	756	871
	Beaver Valley 2	157	1088	392	696
JOILET IL	Braidwood 1	193	2870	1054	1816
	Braidwood 2	193	•	•	•
DECATOR AL	Browns Ferry 1	764	3471	1864	1607
	Browns Ferry 2	764	3471	2116	1355
	Browns Ferry 3	764	3471	1588	1879
SOUTHPORT NC	Brunswick 1	560	1767	984	783
	Brunswick 2	560	1767	1020	747
ROCKFORD IL	Byron 1	193	2781	1278	1503
	Byron 2	193	•	•	•
FULTON, MO	Callaway	193	1340	829	511
ANNAPOLIS, MD	Calvert Cliffs 1	217	1830	1362	468
	Calvert Cliffs 2	217	•	•	•
ROCK HILLS SC	Catawba 1	193	1418	705	622
	Catawba 2	193	1418	686	695
CLINTON, IL	Clinton	624	2515	1124	1381
GLENN ROSE TX	Comanche Peak 1	193	556	765	526
	Comanche Peak 2	193	735	•	•
NEBRASKA CITY, NE	Cooper	548	2366	1340	1026
CRYSTAL RIVER, FL	Crystal River 3	177	1357	680	677
TOLEDO, OH	Davis-Besse	177	718	601	117
BENTON HARBOR MI	D.C. Cook 1	193	3613	2015	1598
	D.C. Cook 2	193	•	•	•
SAN LUIS OBISPO CA	Diablo Canyon 1	193	1324	640	684
	Diablo Canyon 2	193	1317	660	657
MORRIS IL	Dresden 2	724	3537	2562	975
	Dresden 3	724	3536	2380	1156
CEDAR RAPIDS, IA	Duane Arnold	368	2411	1648	763
DOTHAN, AL	Farley 1	157	1407	662	527
	Farley 2	157	1407	593	641

	PLANT NAME	FUEL IN CORE	AVAILABLE SPENT FUEL POOL CAPACITY	FUEL IN SPENT FUEL POOL	REMAINING SPENT FUEL POOL CAPACITY
TOLEDO, OH	Fermi 2	764	2383	1296	1087
OSWEGO, NY	FitzPatrick	560	2797	2080	717
ONAHA, NE	Fort Calhoun	133	1083	706	377
ROCHESTER, NY	Ginna	121	1879	879	435
VICKSBURG, MS	Grand Gulf 1	800	4348	2488	1860
BAXLEY, GA	Hatch 1	560	5946	4884	1062
	Hatch 2	560	•	•	•
WILMINGTON, DE	Hope Creek	764	4006	1708	2298
NEW YORK, NY	Indian Point 2	193	1374	917	457
	Indian Point 3	193	1345	672	655
GREENBAY, WI	Kewaunee	121	990	780	210
OTTAWA, IL	LaSalle 1	764	7932	3076	4852
	LaSalle 2	764	•	•	•
PHILADELPHIA, PA	Limerick 1	764	2832	1701	1131
	Limerick 2	764	3921	1893	2028
CHARLOTTE, NC	McGuire 1	193	1351	871	480
	McGuire 2	193	1425	1039	386
NEW LONDON CT	Millstone 2	217	1306	868	423
	Millstone 3	193	756	416	340
MINNEAPOLIS, MN	Monticello	484	2209	1094	1115
OSWEGO, NY	Nine Mile Point 1	532	2776	2200	576
	Nine Mile Point 2	764	4049	1400	2649
RICHMOND, VA	North Anna 1	157	1737	1505	169
	North Anna 2	157	•	•	•
GREENVILLE, SC	Oconee 1	177	1312	1094	218
	Oconee 2	177	1312	1094	218
	Oconee 3	177	825	552	273
TOMS RIVER, NJ	Oyster Creek	560	2645	2420	180
SOUTH HAVEN, MI	Palisades	204	771	657	101
PHOENIX, AZ	Palo Verde 1	241	1205	648	557
	Palo Verde 2	241	1205	644	561
	Palo Verde 3	241	1205	664	541
LANCASTER, PA	Peach Bottom 2	764	3819	2720	1099
	Peach Bottom 3	764	3819	2777	1042
PAINESVILLE, OH	Perry 1	748	4020	1504	2516

	PLANT NAME	FUEL IN CORE	AVAILABLE SPENT FUEL POOL CAPACITY	FUEL IN SPENT FUEL POOL	REMAINING SPENT FUEL POOL CAPACITY
PLYMOUTH, MA	Pilgrim	580	3859	1974	1885
MANITOWOC WI	Point Beach 1	121	1502	1347	155
	Point Beach 2	121	*	*	*
MINNEAPOLIS MN	Prairie Island 1	121	1386	1237	125
	Prairie Island 2	121	*	*	*
MOLINE IL	Quad Cities 1	724	3657	1933	1724
	Quad Cities 2	724	3897	2943	954
BATON ROUGE, LA	River Bend	624	2680	1400	1280
FLORENCE, SC	Robinson	157	544	302	242
WILMINGTON DE	Salem 1	193	1632	772	850
	Salem 2	193	1632	584	1038
SAN CLEMENTE CA	San Onofre 2	217	1542	870	672
	San Onofre 3	217	1542	918	624
PORTSMOUTH, NH	Seabrook	193	1236	376	860
CHATTANOOGA TN	Sequoyah 1	193	2091	1295	796
	Sequoyah 2	193	*	*	
RALEIGH, NC	Shearon Harris 1 (accepts spent fuel from other units)	157	4184	720 PWR and 1841 BWR	336 PWR and 557 BWR
BAY CITY TX	South Texas 1	193	1969	428	1529
	South Texas 2	193	1969	400	1556
FT. PIERCE FL	St. Lucie 1	217	1706	1128	578
	St. Lucie 2	217	1076	692	384
COLUMBIA, SC	Summer	157	1276	637	567
NEWPORT NEWS VA	Surry 1	157	1044	854	190
	Surry 2	157	*	*	*
BERWICK PA	Susquehanna 1	764	2840	2655	None
	Susquehanna 2	764	2840	1762	823
HARRISBURG, PA	Three Mile Island	177	1338	755	583
MIAMI FL	Turkey Point 3	157	1395	808	587
	Turkey Point 4	157	1389	770	619
BATTLEBORO, VT	Vermont Yankee	368	2863	2331	532
AUGUSTA GA	Vogtle 1	193	1475	1081	2392
	Vogtle 2	193	1998	*	*
RICHLAND, WA	WNP 2	764	2654	1703	951
NEW ORLEANS, LA	Waterford 3	217	2398	700	1698
SPRING CITY, TN	Watts Bar 1	193	1612	80	1530
BURLINGTON, KS	Wolf Creek	193	1327	664	663

* Single values given for multiple units using common fuel storage facility.

00102

Update of Evacuation Time Estimates

August 1, 2001

- Addresses
- Intent
- Background Information
- Summary of Issue
- Backfit Discussion
- *Federal Register Notification*
- Paperwork Reduction Act Statement

Addresses

All holders of operating licenses for nuclear power plants.

TOP

Intent

The U.S. Nuclear Regulatory Commission (NRC) is issuing this Regulatory Issue Summary (RIS) to alert addre: possible need to update emergency planning evacuation time estimates as the results of the year 2000 census published. This RIS does not transmit any new requirements or staff positions. No specific action or written res required.

TOP

Background Information

Addressees are required to follow and maintain in effect emergency plans which meet the standards in Section 50.47(b) and the requirements of 10 CFR Part 50 Appendix E. The requirements concerning emergency plan cl found in Section 10 CFR 50.54(q). This regulation allows a licensee to change its emergency plan without Com approval provided that the change does not decrease the effectiveness of the plan and the plan, as changed, c meet the planning standards of Section 10 CFR 50.47(b) and the requirements of 10 CFR Part 50 Appendix E. evacuation time estimates would not be considered a decrease in the effectiveness of the emergency plan und CFR 50.54(q) and licensees may update the estimates without prior Commission approval.

Additionally, Section IV.G of Appendix E requires licensees to have provisions in these emergency plans to ens emergency plan and its implementing procedures are kept up to date and that emergency equipment and supp properly maintained. Since the emergency plan is contained in the Final Safety Analysis Report in accordance 50 Appendix E Section III, the updating requirements of 10 CFR 50.71(e) apply.

Guidance on evacuation time estimates is in Section J.8, 10l, 10m, and Appendix 4 of NUREG-0654, "Criteria f Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Plants." This guidance was endorsed by NRC Regulatory Guide 1.101, Rev 2. Additional information can be fou NUREG/CR-4831, "The State of the Art in Evacuation Time Estimate Studies for Nuclear Power Plants", March :

TOP

Summary of Issue

Recently published results of the year 2000 census show increases or decreases in population within the plume pathway emergency planning zone around certain nuclear power facilities. Consequently, the estimated times evacuation of the public could increase or decrease. Longer or shorter evacuation times in turn affect decisions evacuating the public in the event of a radiological emergency. Therefore, decision makers may need updated how long it would take to evacuate the public.

TOP

Backfit Discussion

This RIS does not require any action or written response nor does it require any modification to plant structure components or design of facilities; therefore, the staff did not perform a backfit analysis.

TOP

Federal Register Notification

A notice of opportunity for public comment was not published in the *Federal Register* because this RIS is inforr pertains to a staff position that does not represent a departure from current regulatory requirements and prac

TOP

Paperwork Reduction Act Statement

This RIS does not request any information collection.

If you have any question about this matter, please contact the person listed below or the appropriate Office of Reactor Regulation (NRR) project manager.

TOP

/RA Frank P. Gillespie Acting for/

David B. Matthews, Director
Division of Regulatory Improvement Programs
Office of Nuclear Reactor Regulation

Technical contact: Edwin F. Fox, Jr., NRR
301-415-2908
E-mail: eff@nrc.gov

Attachment: List of Recently Issued NRC Regulatory Issue Summaries

---

(ADAMS Accession Number ML012070310)