STATUS REPORT ON FEDERAL AND LOCAL EFFORTS TO SECURE RADIOLOGICAL SOURCES

FIELD HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

SEPTEMBER 14, 2009

Serial No. 111–34

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

54–223 PDF WASHINGTON : 2010

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

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
BILL PASCRELL, JR., New Jersey
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
JAMES A. HIMES, Connecticut
MARY JO KILROY, Ohio
ERIC J.J. MASSA, New York
DINA TITUS, Nevada
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
PETE OLSON, Texas
ANH "JOSEPH" CAO, Louisiana
STEVE AUSTRIA, Ohio

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

YVETTE D. CLARKE, New York, *Chairwoman*

LORETTA SANCHEZ, California
LAURA RICHARDSON, California
BEN RAY LUJÁN, New Mexico
MARY JO KILROY, Ohio
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DANIEL E. LUNGREN, California
PAUL C. BROUN, Georgia
STEVE AUSTRIA, Ohio
PETER T. KING, New York *(Ex Officio)*

JACOB OLCOTT, *Staff Director*
DR. CHRIS BECK, *Senior Advisor for Science and Technology*
DANIEL WILKINS, *Clerk*
COLEY O'BRIEN, *Minority Subcommittee Lead*

CONTENTS

STATUS REPORT ON FEDERAL AND LOCAL EFFORTS TO SECURE RADIOLOGICAL SOURCES

Monday, September 14, 2009

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY,
Brooklyn, NY.

The subcommittee met, pursuant to call, at 9:55 a.m., in the SUNY Downstate Alumni Auditorium, Brooklyn, New York, Hon. Yvette D. Clarke presiding.

Present: Representatives Clarke, Sanchez, Richardson, and Lungren.

Ms. CLARKE. The subcommittee will come to order.

Good morning. I would like to welcome you all to Brooklyn this morning and thank the Members of the subcommittee—Mr. Lungren, the Ranking Member; Ms. Sanchez; and Ms. Richardson—for travelling from your own districts to participate in today's hearing.

Today's hearing is entitled, "Status Report on Federal and Local Efforts to Secure Radiological Sources." Radiological source security is essential in preventing a radiological dispersed device, or RDD, often called a "dirty bomb." To put it simply: No radiological material, no dirty bomb.

Two years ago, this subcommittee, along with members of the New York City delegation, came to New York to observe some of the early efforts to secure radiological sources, specifically those cesium chloride sources found in hospital blood irradiators.

At that time, those early efforts were spearheaded by a partnership effort between New York City and the Brookhaven National Laboratory. Security measures, such as closed-circuit television cameras, keypad locking systems with alarms, and other access controls, were being put in place.

Over the next 2 years, three Federal agencies—the Department of Homeland Security's Domestic Nuclear Detection Office, DNDO; the Department of Energy's National Nuclear Security Administration, NNSA; and the Nuclear Regulatory Commission, NRC—continued this idea by looking at the risk posed by the cesium chloride sources and proposing some solutions.

These efforts became a little more sophisticated and brought the security focus closer to the source. The three agencies decided to take three actions to better secure radiological sources: No. 1, harden blood irradiators to make it more difficult to remove the

CSCL sources called "engineering upgrades"; examine whether alternate sources besides cesium chloride could be used; and, No. 3, improve the licensing and tracking system for sources.

So today we are here to get an update on these efforts, and we have an exceptional panel of witnesses to help us in our efforts.

From the Department of Homeland Security, Mr. Craig Conklin is the director of the Sector-Specific Agency Executive Management Office, Office of Infrastructure Protection.

Welcome.

From the Department of Energy, Mr. Kenneth Sheely is the associate assistant deputy director for global threat reduction, National Nuclear Security Administration.

Welcome.

From the Nuclear Regulatory Commission, Mr. Robert Lewis is the director of the Division of Materials Safety and State Agreements, MSSA.

Welcome.

These three Federal witnesses will tell us about their current efforts, what has worked, what hasn't, and their future plans.

Next we have Captain Michael Riggio, the director of counterterrorism at the New York Police Department.

Welcome.

We also have Mr. Gene Miskin, the director of the Office of Radiological Health for the New York City Department of Health and Mental Hygiene.

Welcome.

The New York Police Department and public health departments have been forward-thinking and aggressive in their efforts to secure these sources. They have also shown us that police and public health, two entities who don't see eye-to-eye very often, can work together to achieve a common goal. We are also interested in hearing from them how the various Federal agencies have worked with them.

Also from New York is Dr. Bonnie Arquilla, who is the director of disaster preparedness here at SUNY Downstate Medical Center.

Thank you for being here, and thank you to SUNY Downstate for allowing us to hold this hearing here.

Finally, from the Government Accountability Office is Mr. Gene Aloise, the director of the Natural Resources and Environment Division.

Dr. Arquilla and Mr. Aloise will not speak directly to the source security efforts specifically but will provide helpful context. Dr. Arquilla will explain the kinds of efforts and activities that would be necessary to respond to an RDD event. Mr. Aloise will discuss the activities that would be involved in recovering from such events.

I think we will all see that both response and recovery are quite difficult and expensive. We should be doubly motivated to ensure that the radiological sources are as well-protected as possible.

I believe in this mission. After the trip I mentioned 2 years ago, I introduced the Radiological Materials Security Act, which was reintroduced in April of this year. The provisions of the bill provide for the three Federal agencies here to carry out the activities that they have been and continue to carry out in their trilateral efforts.

Although the bill has not yet been passed, it has helped me to push for the appropriations to keep radiological source security and detection efforts going. I hope that the bill and this field hearing make it clear to the witnesses here today, as well as the agencies and departments that you represent, that Congress has an interest in your efforts. We will support you, and we want to see progress.

Thank you for being here. I look forward to your testimony and the following discussion.

I now recognize the Ranking Member, Dan Lungren of California, for an opening statement.

Mr. LUNGREN. Thank you very much, Madame Chairwoman.

In the interest of time, I would ask unanimous consent that my prepared opening statement be included in the record.

Ms. CLARKE. So ordered.

Mr. LUNGREN. With that, I would just say, thank you, all of you, for being here. I appreciate it. One thing I have learned already is that, on the Federal level, we obviously have the corner on longer titles than the rest of the Government. It is a mouthful.

I realize this is an extremely important issue. I thank all of you for being here. I particularly am interested not only in the prevention and the recovery, but also that we do a better job of getting information out to the public exactly what a dirty bomb is, so that we might be able to understand how to respond to that and also diminish some of the panic that seems to ensue with every discussion of dirty bombs.

Not that they are not important, but that we understand what they can do and what they cannot do will help us to be able to respond in a far better way than I think we are prepared to do right now.

With that, I would yield back the balance of my time.

Ms. CLARKE. I now recognize the gentlelady from California, Ms. Loretta Sanchez of California, for an opening statement.

Ms. SANCHEZ. Madam Chairwoman, in the interest of time, we will submit something for the record.

I just wanted to let you know that you have three Californians joining you today here in New York City, and that is because we share so much interest in this, as major metropolitan areas, both on the East and the West Coast.

We look forward to the testimony. We think it is an important issue. So I thank you.

Ms. CLARKE. Thank you very much.

I now recognize the gentlelady from California, Laura Richardson of California, for an opening statement.

Ms. RICHARDSON. Thank you, Madame Chairwoman.

First of all, I would like to take this opportunity to thank you for convening this hearing. This is a very important subject that we need to stay diligent on. We do appreciate your leadership on this matter.

I would like to briefly share with you, in addition to being on the committee, the reason why I found it of importance and wanted to participate. I represent the area of Long Beach, California, where one block out of my district is the entire port complex which is the port of Long Beach and the Port of Los Angeles, which is the largest port in the United States.

When we consider this discussion, it is of much concern to us, of all the people, 16 million people, who live within a certain radius who could be very inevitably affected if we were to have a situation such as we are discussing this morning.

But I just want to say thank you in advance to all the witnesses for coming and preparing and providing us with the information that we need so we can legislate in a more effective way.

Thank you very much.

Ms. CLARKE. Thank you.

In the interest of time, I will ask that each of you provide a brief biography of your work. Without objection, the witnesses' full statements will be entered into the record. Hearing no objection, so ordered.

I now ask each witness to introduce yourself and summarize your statement for 5 minutes, beginning with Mr. Conklin.

STATEMENT OF CRAIG CONKLIN, DIRECTOR, SECTOR-SPECIFIC AGENCY EXECUTIVE MANAGEMENT OFFICER, OFFICER OF INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY

Mr. CONKLIN. Thank you. My name is Craig Conklin. I am director of the Sector-Specific Agency Executive Management Office within the Department of Homeland Security.

Good morning, Chairwoman Clarke, Ranking Member Lungren, and distinguished Members of the subcommittee. I appreciate the opportunity to testify on the Department of Homeland Security's and the Federal Government's efforts to enhance the security of radiological sources and ensure that they are not used in a manner that is hostile to the United States.

Under Homeland Security Presidential Directive 7, the Office of Infrastructure Protection leads a coordinated national program to reduce risk to the Nation's critical infrastructure and key resources and to strengthen National preparedness, timely response, and a rapid recovery of these assets in the event of an attack, natural disaster, or other emergency.

These risk-mitigation efforts are accomplished using the partnership framework established in the National Infrastructure Protection Plan. This plan brings together all levels of government, the private sector, nongovernmental organizations, and international partners to enhance sector security resiliency.

My office was assigned sector-specific agency responsibilities for six of the 18 critical infrastructure sectors, including the nuclear sector. The nuclear sector-specific agency facilitates and implements programs that help achieve security by effectively reducing vulnerabilities and consequences of attack using risk-based assessments, industry best practices, protective measures, resiliency strategies, and comprehensively sharing information between industry and all levels of government.

Our government partners include, among others, the National Nuclear Security Administration, the Nuclear Regulatory Commission, and the Federal Bureau of Investigation, as well as officials from the States of Delaware, Florida, Massachusetts, Pennsylvania, and Texas.

Our private-sector partners include representatives from the commercial nuclear power industry, producers and users of radioactive sources, universities that operate research and test reactors, and radioactive material shippers.

While our efforts run the gamut of the nuclear sector, today I will briefly describe four efforts to protect portable radioactive sources.

First, in 2007, we formed a Radioisotope Subcouncil to address radioactive source security concerns. The purpose of the subcouncil is to identify and recommend measures to prevent sources of concern from being stolen and used as a radiological dispersal device or a radiological exposure device.

In late 2008, the subcouncil conducted a radioactive source security workshop, which identified three issues for further examination: First, the potential risk presented by limited commercial disposition of sealed sources; second, the use of commercial, off-the-shelf technologies to track conveyances, packages, and sources during transport; and, third, reconciliation of the sometimes confusing regulations covering the transportation of radioactive sources.

A focus group has been created to address each of these issues. The removal and disposal focus group will develop a concise message on the potential national security concerns caused by the lack of commercial disposition options for these sealed sources and will investigate immediate and long-term options to address that concern.

The tracking focus group will develop a position paper on the pros and cons and cost-effectiveness of the identified tracking technologies. The transportation focus group will establish an approved definition for "transit" and "transshipments" and develop an action plan for addressing any regulatory gaps and/or inconsistencies in the transportation regulations.

Second, the Nuclear Sector-Specific Agency, in close coordination with its Federal partners, maintains and regularly updates a matrix of Federal programs and initiatives that are being implemented to enhance source security. The purpose of this matrix is to help reduce duplication of efforts, maximize the use of limited Federal resources, and identify gaps in Federal activities. The matrix currently tracks 26 Federal initiatives.

Third, the Department of Homeland Security's Domestic Nuclear Detection Office is also actively engaged in a number of source security initiatives. DNDO is leading the Securing the Cities Initiative effort to design and implement architecture for a coordinated and integrated preventive detection and interdiction of illicit radiological materials that may be used a weapon within a high-risk urban area.

It is also chairing the Public Education Subgroup of the NRC-led Radioactive Source Task Force designed to enhance the general knowledge of the public concerning radiological dispersal devices.

Finally, DNDO is leading a small-business initiative research program to promote the design and production of non-nuclear alternatives for industrial devices that use radioactive sources.

The last effort I would like to describe is our information sharing through the trilateral meetings. The Department of Homeland Security, the NRC, and NSA participate in these meetings. The tri-

lateral meetings provide an informal forum to discuss on-going projects regarding radioactive source security. The purpose is to avoid and minimize surprises with other agencies' activities and provide an efficient and effective path forward to enhance source security. We hold these meetings on a quarterly basis.

In closing, the Office of Infrastructure Protection works closely with its Federal, State, local, territorial, and Tribal and private-sector partners within the nuclear sector to ensure the protection and resiliency of the sector.

I will be glad to respond to any questions the subcommittee may have.

[The statement of Mr. Conklin follows:]

PREPARED STATEMENT OF CRAIG CONKLIN

SEPTEMBER 14, 2009

Good morning Chairwoman Clarke, Ranking Member Lungren, and distinguished Members of the subcommittee. As Director of the Sector-Specific Agency Executive Management Office (SSA EMO) in the Department of Homeland Security's (DHS') Office of Infrastructure Protection, I appreciate the opportunity to discuss the Federal Government's coordinated effort to secure radioactive sources and ensure that they are not used in a manner hostile to the United States. I will also highlight how the Federal Government continues to work with our State, local, Tribal, and private sector partners to execute this important mission.

Under Homeland Security Presidential Directive 7 (HSPD–7), Critical Infrastructure Identification, Prioritization, and Protection, the DHS Office of Infrastructure Protection leads a coordinated National program that aims both to reduce risks to the Nation's critical infrastructure and key resources (CIKR) as well as to strengthen the preparedness, response, and recovery of these assets in the event of an attack, natural disaster, or other emergency. These risk mitigation efforts are accomplished through the collaborative framework established in the National Infrastructure Protection Plan (NIPP), which brings together all levels of government, the private sector, non-governmental organizations, and international partners in support of this CIKR protection and response mission.

In the context of the NIPP, CIKR protection includes actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other man-made or natural disaster. Protection can include a wide range of activities such as:

- improving security protocols;
- hardening facilities;
- building resiliency and redundancy;
- incorporating hazard resistance into facility design;
- initiating active or passive countermeasures;
- installing security systems;
- leveraging "self-healing" technologies;
- promoting workforce surety programs;
- implementing cybersecurity measures;
- training and exercises; and
- business continuity planning.

Recognizing that each CIKR sector possesses its own unique characteristics, HSPD–7 designates Federal Government Sector-Specific Agencies (SSAs) for each of the 18 CIKR Sectors. The SSAs are responsible for: Implementing the NIPP sector partnership model and risk management framework; developing protective programs and resiliency strategies; and providing sector-level CIKR protection guidance in line with the overarching NIPP framework established by DHS pursuant to HSPD–7.

The SSA EMO was assigned SSA responsibilities for six of the 18 CIKR Sectors: Chemical; Commercial Facilities; Critical Manufacturing; Dams; Emergency Services; and Nuclear Reactors, Material, and Waste. The SSA facilitates and implements programs that help achieve security by reducing vulnerabilities and consequences of attack through risk-based assessments, industry best practices, protective measures, and comprehensive information sharing between industry and all levels of government. The remainder of this testimony will focus on the Nuclear Reactors, Material, and Waste Sector.

The Nuclear Reactors, Material, and Waste Sector is comprised of:
- Nuclear Power Plants—104 power reactors at 65 sites;
- Research and Test Reactors—32 reactors in 22 States;
- Radioisotopes—portable sources primarily for medical and industrial use;
- Twenty-eight irradiation facilities;
- Twelve major manufacturers/distributors of radioactive sources;
- Eight major fuel fabrication and production facilities;
- Six spent fuel storage facilities;
- Four mixed-waste facilities; and
- One uranium hexafluoride production facility.

As the lead Federal coordinator, the role of the Nuclear SSA within the Nuclear Reactors, Material, and Waste Sector (herein referred to as the Nuclear Sector) is to build and sustain relationships with Government and private sector security partners to coordinate the identification, prioritization, and protection of Nuclear Sector CIKR. HSPD–7 directs the Secretary of Homeland Security to "continue to work with the Nuclear Regulatory Commission (NRC) and, as appropriate, the Department of Energy in order to ensure the necessary protection [of the Nuclear Sector]." This entails: Maintaining the *Sector Specific Plans for CIKR Protection in the Nuclear Sector* and submitting the corresponding *Annual Sector CIKR Protection Report for the Nuclear Sector;* assessing sector-level performance to enable protection-program gap assessments; identifying protection priorities; coordinating and supporting risk assessments and management programs for high-value CIKR; and supplying sector-specific CIKR information for incident response, among other responsibilities.

Critical infrastructure protection and resiliency are the shared responsibilities of Federal, State, local, Tribal, and territorial governments, regional coalitions, and the private sector owners and operators of the Nation's CIKR. The NIPP relies on a partnership model as the primary organizational structure for coordinating CIKR efforts and activities, encouraging the formation of Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs). The SCCs and corresponding GCCs work in tandem to create a coordinated National framework for CIKR protection and resiliency within and across sectors.

As Director of the SSA EMO, I chair the Nuclear Sector's Nuclear Government Coordinating Council (NGCC). The NGCC is the Principal Federal interagency body responsible for working with public and private partners to coordinate and implement civilian nuclear security strategies, activities, and policies; facilitate relevant communications across the Government and between the Government and the private sector; and coordinate with the emergency management and public health and safety communities regarding response and recovery issues associated with a terrorist act. The NGCC's membership consists of representatives from DHS, National Nuclear Security Administration (NNSA), Nuclear Regulatory Commission (NRC), Federal Bureau of Investigation (FBI), Department of Energy (DOE), Department of State, Department of Transportation, Environmental Protection Agency, along with officials from the radiation-control programs in the States of Delaware, Florida, Massachusetts, Pennsylvania, and Texas. The NGCC's work encompasses CIKR protection activities at the full range of Nuclear Sector assets.

The role of the Nuclear Sector's Nuclear Sector Coordinating Council (NSCC) is to provide a mechanism through which the nuclear industry may provide input into nuclear CIKR protection policy development and implementation; further, it provides a forum for companies and key organizations involved in nuclear security issues to cooperate with Government on nuclear CIKR protection. The NSCC is comprised of representatives from nuclear power reactor operators, fuel manufacturing facilities, nuclear reactor manufacturers, nuclear waste management/transportation companies, nuclear trade associations, the Nuclear Energy Institute and the National Organization of Test, Research, and Training Reactors.

The Critical Infrastructure Partnership Advisory Council (CIPAC) directly supports the sector partnership model by providing a legal framework that enables members of the NSCC and NGCC to engage in joint CIKR protection-related discussions. DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC as a Federal Advisory Committee Act-exempt body, pursuant to Section 871 of the Homeland Security Act.

The Nuclear Sector's mission statement declares that "the Nuclear Sector will support national security, public health and safety, public confidence, and economic stability by enhancing, where necessary and reasonably achievable, its existing high level of readiness to promote the security of the Nuclear Sector, and to lead by example to improve the Nation's overall critical infrastructure readiness." In furtherance of this mission, the Nuclear CIPAC agreed on eight security goals for the partnership to pursue above and beyond existing regulation:

Awareness

- *Goal 1*.—Establish permanent and robust collaboration and communication among all stakeholders having security and emergency response responsibilities for the Nuclear Sector.
- *Goal 2*.—Obtain information related to other CIKR assets' dependencies and interdependencies with the Nuclear Sector and share it with sector security partners.
- *Goal 3*.—Increase public awareness of sector protective measures, consequences, and proper actions following a release of radioactive material.

Prevention

- *Goal 4*.—Improve security, tracking, and detection of nuclear and radioactive material in order to prevent it from being used for malevolent purposes.
- *Goal 5*.—Coordinate with Federal, State, and local law enforcement agencies to develop protective measures and tactics to deter, detect, and prevent terrorist attacks on nuclear facilities and other Nuclear Sector assets.

Protection, Response, and Recovery

- *Goal 6*.—Protect against exploitation of the Nuclear Sector's cyber assets, systems, networks, and the functions they support.
- *Goal 7*.—Use a risk-informed approach that includes security considerations to make budgeting, funding, and grant decisions on all identified potential protection and emergency response enhancements.
- *Goal 8*.—Enhance the ability of Federal, State, territorial, local, and Tribal governments and the private sector to effectively respond to nuclear and radiological emergencies that result from terrorist attacks, natural disasters, or other incidents.

DHS formed three Sub-councils within the NIPP Framework, meeting under the CIPAC, which are the Cyber, Research and Test Reactor, and Radioisotopes Subcouncils. I would like to take the opportunity to highlight a few examples of the public-private partnership under the NIPP.

Comprehensive Reviews

Comprehensive Reviews (CRs) were security assessments conducted at all 65 nuclear power sites between May 2005 and September 2007, with the Final Integrated Protective Measures Analysis Report issued in March 2008. The process provided a vehicle for discussion with stakeholders on potential enhancements to security in and around the sites. This framework assisted in reducing vulnerabilities, implementing appropriate protective measures, and mitigating the potential consequences of a successful attack. The Office of Infrastructure Protection's Protective Security Coordination Division and the SSA EMO led the CR teams, which included representation from Federal agencies such as the U.S. Coast Guard (which participated in the 49 CRs that had a water nexus), Federal Emergency Management Agency (FEMA), FBI, Transportation Security Administration, DHS National Cyber Security Division, and NRC. The Federal teams worked cooperatively with the State Homeland Security Advisor; State, county, and local emergency managers and planners and emergency response agencies; and private representatives and associations. Following each visit, the CR team analyzed the information and shared it with appropriate stakeholders, which included Federal agencies, State and local law enforcement, emergency management organizations, and facility owners and operators.

Comprehensive Review Outcomes Working Network

The Comprehensive Review Outcomes Working Network (CROWN) project was established to systematically follow up on the approximately 1,800 potential enhancements identified during Nuclear Sector CRs. The process has resulted in tangible security improvements and has also enabled the Nuclear Sector partners to cultivate and sustain strong working relationships with the Office for Bombing Prevention, the Office of Emergency Communications, the Office of Interoperability and Capability, and FEMA's National Integration Center.

Research and Test Reactor Security Enhancement Project

The Research of Test Reactor (RTR) Security Enhancement Project is a voluntary, cooperative initiative at the request of the RTR community to explore opportunities to perform security upgrades at RTR facilities. Physical security enhancements have been completed at the Universities of Missouri—Columbia and Oregon State nuclear research and test reactors. The security enhancement program originated in the NSCC and was implemented through partnership among the NRC, NNSA, DHS, and the RTR community. Improvements include installing new alarm communica-

tion systems, displays with closed-circuit television recording capability, airlock door enhancements, and hardened entry gates and access points. Due to the success of these first two pilot projects, the program will be expanded to include approximately eight additional facilities.

Blood Irradiator In-Device Delay Program

The Blood Irradiator In-Device Delay (IDD) Program is an initiative to significantly increase the time needed for unauthorized removal of the radioactive source from blood irradiators, which represent significant sources of radioactive material. The scope of this initiative includes 843 of an estimated 1,000 cesium irradiators in the United States, with NNSA overseeing the IDD effort for all three major irradiator manufacturers (Best Theratronics, Ltd. (BTL)—GC40, GC1000, GC3000; Pharmalucence/CIS—IBL 437; and JL Shepherd & Associates (JLSA)—JL Mark 1). This initiative has been endorsed by the Organization of Agreement States, NRC, and DHS. National implementation of the IDD Program is presently under way. As of June 2009, 25 kits have been installed, with installations for existing devices projected through 2016. New blood irradiators will have the security enhancements installed at the factory before customer delivery.

The Radioisotopes Sub-council specifically addresses radioactive source security concerns by developing and recommending policies, strategies, plans, and measures to enhance the physical security and emergency preparedness of the Nation's radioisotope sector. The Radioisotopes Sub-council focuses in particular on identifying and recommending measures to prevent radioisotopes of concern from being stolen, diverted, and used in Radiological Dispersal Devices, Radiation Exposure Devices, or for other malicious purposes. At the request of the NSCC Chair, the NGCC held a Radioactive Source Security Workshop Sept. 16–17, 2008, to prioritize and identify areas on which to focus the energy and resources of the Radioisotopes Sub-council. The facilitated workshop included over 50 public and private-sector attendees. Workshop participants identified three source security issues which warranted further examination:

1. Potential national security concerns presented by the lack of commercial disposition options for sealed radiation sources (e.g., radiography sources).
2. The capacity for existing commercially available off-the-shelf technologies to physically track conveyances, packages, and sources during transport.
3. Reconciliation of the myriad, and sometimes confusing, relevant regulatory authorities and associated security regulations integral to the transport, transportation, and transshipment of Category 1 and 2 sources as defined by the International Atomic Energy Agency.

Federal and State officials are now working through the Radioisotopes Sub-council and its private-sector equivalent to better understand the scope and scale of these issues. As a result, three Focus Groups have been created to address these three issues.

The Removal and Disposal of Disused Sources Focus Group identifies removal and disposition options for disused sources. Currently, the limited number of commercial disposal pathways and recycling options could lead to sites stockpiling disused sources. The Focus Group will develop a concise message on the potential national security concern caused by the lack of commercial disposition options for disused sealed sources and investigate immediate and long-term options to address the concern (e.g., incentives to open commercial facilities to waste not generated within the boundaries of their waste compacts and incentives for consolidated interim storage) by October 2009.

The Tracking of Radioactive Sources Focus Group compiles technical specifications of commercially available passive and active tracking systems and subsequently evaluates the identified technology relevant to its capability for tracking conveyances, packages, or sources. The Focus Group will culminate its initial efforts with a position paper by November 2009 on the pros, cons, and cost-effectiveness of each identified technology.

The Transportation of Radioactive Sources Focus Group identifies relevant regulatory authorities and associated transportation security regulations to reconcile and analyze the overlaps, gaps, and potential inconsistencies in those Federal transportation security regulations. Additionally, this Focus Group will seek to establish an inter-governmentally approved definition for transit and transshipment, to include an action plan with a set of recommendations for addressing any regulatory gaps and/or inconsistencies by December 2009.

The Nuclear SSA, in close coordination with its Federal partners, maintains and regularly updates a matrix of Federal programs and initiatives to promote the security of radiation sources. The "Source Security Matrix" tracks dozens of Federal programs and initiatives to address the risk that domestic U.S. radioactive sources

poses; it is updated monthly, issued quarterly, and remains a continuing agenda item at the Nuclear Sector's quarterly meeting. The purpose of this matrix is to help reduce duplication of effort, maximize the use of limited Federal resources, and identify gaps in Federal activities.

In addition to the efforts described above, DHS' Domestic Nuclear Detection Office (DNDO) is actively engaged in a myriad of initiatives with the Nuclear Sector. The Mission of DNDO is to improve the Nation's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the United States.

DNDO addresses source security through its Securing the Cities Initiative, which designs and implements architecture for coordinated and integrated preventative detection and interdiction of illicit radiological materials that may be used as a weapon within a high-risk urban area. The New York City (NYC) Tri-State Region Source Security Subgroup, chartered as part of the NYC Securing The Cities pilot effort, is focused on developing an effective, risk-based approach to increase the security of industrial and medical sources in NYC and the surrounding areas of New York, New Jersey, and Connecticut. The sub-group is:

- Developing a best practices in source security report;
- Performing security reviews of high-risk materials licensees; and
- Evaluating the current notification and tracking system for the movement of sources in the NYC Tri-State area.

DNDO also chaired the Public Education Subgroup as part of the NRC-chaired Radiation Source Security and Protection Task Force to enhance the general knowledge of the public concerning Radioactive Dispersal Devices (RDDs). The subgroup developed an action plan that, when implemented across the Nation, will raise public awareness of the effects of an RDD. It is hoped that this increased public awareness will lower the public panic in response to an actual or perceived RDD event. By mitigating fear and panic of RDDs, it is hoped that either RDDs will become a less attractive weapon of choice for terrorists, or, in the case of an RDD attack, will limit social and economic damage due to an informed public response.

DNDO's Small Business Innovative Research Program (SBIR), implemented in coordination with the DHS Homeland Security Advanced Research Projects Agency, is an effort to promote the design and production of non-nuclear alternatives for industrial devices that use radioactive sources. This program gives seed money to companies who have shown promising designs through a Nation-wide competition. Currently, DNDO has three SBIR contracts.

DNDO's State and Local Stakeholder Working Group supports non-Federal members of the preventative radiological and nuclear detection (PRND) community. DNDO has developed a PRND Program Management Handbook, and over 7,400 law enforcement, first responder personnel, and public officials have completed the agency's five-course training curriculum.

In an effort to share information on source security issues of mutual interest, DHS, NRC, and NNSA participate in what is known as Tri-Lateral Meetings. Tri-Lateral Meetings seek to:

- Discuss issues of mutual interest to participating agencies regarding radiological and nuclear material;
- Avoid or minimize surprises about other agencies' activities;
- Develop an efficient and effective path forward to enhance efforts on source security; and
- Speak with one Federal voice, especially for Congressional and media inquiries.

The Tri-lateral Meetings are held on a quarterly basis, for 2 hours, to share information and discuss agency programs on radiological source security and preparedness matters. The Tri-Lateral Meetings provide an informal information-sharing forum for DHS, NNSA and the NRC to synchronize radiological source security efforts that are not already covered through other established public-private and inter-agency auspices (e.g., NGCC/CIPAC, Radiation Source Protection and Security Task Force). Both DNDO and Infrastructure Protection represent DHS at the Tri-Lateral Meetings, where each participating agency alternates chairing and coordinating the periodic meetings to include logistics and agenda development.

In closing, the Office of Infrastructure Protection works closely with its Federal, State, local, territorial, and Tribal and private-sector partners within the Nuclear Sector to ensure the protection and resiliency of the sector. I would be glad to respond to any questions the subcommittee may have.

Ms. CLARKE. Thank you, Mr. Conklin.

Mr. Sheely.

STATEMENT OF KENNETH SHEELY, ASSOCIATE ASSISTANT DEPUTY ADMINISTRATOR FOR GLOBAL THREAT REDUCTION, NATIONAL NUCLEAR SECURITY ADMINISTRATION, DEPARTMENT OF ENERGY

Mr. SHEELY. Yes, hi. My name is Ken Sheely, from the U.S. Department of Energy's National Nuclear Security Administration.

Chairwoman Clarke and Members of the subcommittee, thank you for giving me this opportunity to testify today on the role that the NNSA Global Threat Reduction Initiative plays in improving security on high-risk radioactive sources.

The GTRI mission is to reduce and protect vulnerable nuclear and radiological material located at civilian sites world-wide. To achieve this mission, GTRI is working in over 100 countries to convert, remove, and protect nuclear and radiological materials. For today's hearing, I will focus my remarks on our efforts to enhance security of radioactive sources in the United States.

To better understand the potential RDD risk, GTRI has completed three studies: One on the economic impacts of an RDD; one to determine the isotopes of concern in the threshold quantities of an RDD of national significance; and the third, co-sponsored with DNDO, to look at the vulnerabilities of cesium chloride irradiators.

These findings, coupled with the open environments of hospitals and universities, make the security at these facilities challenging. To address these challenges, GTRI and the DOE laboratories provide technical expertised based on implementing security best practices at over 600 buildings world-wide.

The GTRI voluntary secure enhancements complement and do not replace NRC's increased controls. In fact, NRC has issued regulatory information summaries to their licensees describing and endorsing GTRI's efforts. GTRI has also been endorsed by DHS, FBI, and the Agreement States.

The first element of GTRI's voluntary security efforts are source recoveries. Since 1997, GTRI's Offsite Source Recovery Project has removed more than 22,000 unwanted sources, totalling more than 700,000 curies in the United States.

The second component of GTRI's security efforts are delay enhancements. For example, as a result of the cesium chloride irradiator vulnerability study, GTRI, DNDO, and NRC, along with manufacturers, developed the in-device delay hardening kits. In August 2008, a pilot program was launched, and the first volunteers included the sites in New York, New Jersey, and Pennsylvania. In May 2009, DNDO transferred their portion of the project to GTRI in order to consolidate all activities under one Federal agency for national implementation since many of these sites have irradiators from more than one of the three vendors. To date, kits have been installed on 32 irradiators. In addition, the vendors have agreed that new kits coming off the production line will have the kits already installed.

In addition to these hardening kits, GTRI enhancements also include other delay devices, such as tie-downs, locks, and hardened doors.

Another component is detection, and the most important element of GTRI's detection features is remote monitoring. This is because, at many hospitals and universities, the alarms would be handled

by 9–1–1 operators who would have lesser understanding of why a cesium irradiator warrants an emergency response. GTRI's remote monitoring addresses this by simultaneously sending prioritized alarms directly to multiple locations, such as the local law enforcement, to ensure timely response.

GTRI security upgrades also include response training. GTRI has developed a unique training course to provide local law enforcement with hands-on training in a realistic setting with actual radioactive sources. To date, we have conducted over six training courses for 175 responders.

As a capstone to our support, NNSA has partnered with the FBI to provide tabletop exercises. The purpose of these exercises is to provide a no-fault site-specific scenario to promote team building and to prepare integrated response plans with Federal, State, local, and private-sector partners. To date, four tabletop exercises have been conducted.

The ultimate risk reduction would be to replace radioactive sources with nonradioactive alternatives. NNSA is currently funding research into technologies such as X-rays for blood irradiation.

Through our security efforts world-wide, we have learned several important lessons. Paramount among them is that a well-trained, well-equipped, and timely response is one of the most important elements in ensuring security. That is why GTRI has concentrated the majority of our voluntary security enhancements on helping these dedicated first responders, from our remote monitoring systems which ensure they receive timely alarms, to the realistic training which ensures they are prepared. In addition, GTRI serves as a conduit to share lessons learned from site to site, city to city, and State to State.

In closing, I am proud to report that GTRI, working in concert with our Federal, State, local, and private-sector partners, has helped to further enhance the security of radioactive sources.

[The statement of Mr. Sheely follows:]

PREPARED STATEMENT OF KENNETH SHEELY

SEPTEMBER 14, 2009

I. INTRODUCTION

Chairwoman Clarke, Ranking Member Lungren and Members of the subcommittee, thank you for giving me the opportunity to testify on the role that the National Nuclear Security Administration's (NNSA) Global Threat Reduction Initiative (GTRI) plays in further improving the security on high-risk radioactive sources. GTRI's mission is to reduce and protect vulnerable nuclear and radiological materials located at civilian sites world-wide. These efforts are focused on the first line of defense, namely securing or removing vulnerable nuclear and radiological material at their source. GTRI has three goals that provide a comprehensive approach to achieving its mission and denying terrorists access to nuclear and radiological materials:

1. CONVERT research reactors and isotope production facilities from the use of highly enriched uranium (HEU) to low enriched uranium (LEU);
2. REMOVE and dispose of excess nuclear and radiological materials;
3. PROTECT high-priority nuclear and radiological material from theft and sabotage.

To achieve its mission, GTRI is working in over 100 countries. For today's hearing I will focus my remarks on GTRI's efforts that are aimed at further enhancing the security of radioactive sources located in the United States that could potentially be used in a radiological dispersal device (RDD) or "dirty bomb." I will begin by describing our approach to defining and prioritizing the risks from radiological mate-

rials. From there I will describe the programs GTRI is leading to mitigate these risks, our efforts to coordinate with Federal, State, and local agencies and the private sector, and lessons we have learned to improve radiological security.

II. RADIOLOGICAL RISKS

The attacks of September 11, 2001, heightened the Nation's concerns regarding the potential use of radioactive materials in a terrorist act. The possibility of such an attack has been of particular concern because of the widespread use and availability of radioactive materials in the United States and abroad by industry, hospitals, and academic institutions. Loss or theft of such materials, in risk-significant quantities, could lead to their diversion for malicious use in an RDD.

An RDD is a device or mechanism that is intended to spread radioactive material from the detonation of conventional explosives or other means. An RDD detonation would likely result in a few deaths (mainly from the explosion), but significant social and economic impacts could result from public panic, decontamination costs, and denial of access to the area for extended periods of time.

To better understand the potential consequences of malevolent use of radiological materials, the specific isotopes of concern, and the vulnerabilities of devices using these materials, GTRI commissioned three key studies to examine these issues in depth. These studies formed the basis for GTRI's voluntary security enhancement efforts and have been shared with our Federal partners.

II.A Economic Impacts

GTRI commissioned an economic impact study to better understand the likely economic disruption were an RDD to be detonated in a major metropolitan area. A joint study by Los Alamos National Laboratory and Sandia National Laboratory prepared for GTRI modeled the impacts of four specific radioactive sources in amounts normally found in devices commonly used in their respective industry. Even without weaponization of the radioactive materials or optimization of the device the study found that the economic cost to the Nation could be in the billions of dollars.[1] Costs included evacuation, relocation, clean-up, and lost wages.

II.B Material of Concern

Although any amount of radioactive material could cause public panic, GTRI's focus is on radiation sources that could be used by a terrorist to cause a significant impact. A second GTRI study tasked Sandia National Laboratories with developing a down-selection methodology that used a rigorous and reproducible process to identify, prioritize, and determine threshold quantities of radioactive materials that could be used in a RDD of national significance.

This "down-selection study"[2] began by examining the comprehensive list of nuclides to ensure all were considered. The first step was to eliminate all stable, i.e., nonradioactive, nuclides. The list was then culled according to half-life and specific activity. Shorter-lived nuclides likely would not be effectively used in an RDD because they would decay away too quickly. Nuclides with half-lives greater than 100,000 years were also not of concern because the mass of material required for a significant RDD would be excessively large, making use and dispersion of these materials very difficult. The final step was to identify radionuclides that are commercially available to end-users world-wide or may be available in bulk quantities to a limited number of suppliers and manufacturers in quantities greater than 0.1 curie (alpha emitters) and 1 curie (beta/gamma emitters). The final result was 14 radionuclides and spent fuel that GTRI determined could be used to make a significant RDD and were candidates for voluntary security enhancements.

The 14 radionuclides documented in the down-selection report include isotopes in wide commercial and medical use in the United States. The GTRI-funded study was subsequently used by the Radiation Source Protection and Security Task Force, Chaired by the Nuclear Regulatory Commission (NRC), to develop the interagency cleared report of July 8, 2009, *Reevaluation of the List of Radioactive Sources That Warrant Enhanced Security and Protection and Quantities of Radioactive Material Sufficient to Create a Significant Radiological Dispersal Device or Radiation Exposure Device.* In addition, a study by the National Academy of Sciences identified Ce-

---

[1] *Economic Impacts of Detonating Radiological Dispersion Devices,* Los Alamos National Laboratory, February 15, 2008, LA–CP–08–00973.

[2] *Radioactive Material Downselection and Source Prioritization Methodology,* Sandia National Laboratory, November 21, 2008.

sium Chloride (CsCl) as posing a greater concern than the other radionuclides because it is widely used in significant quantities and is soluble and dispersible.[3]

II.C Cesium Irradiator Vulnerabilities

The third study sponsored by GTRI and co-sponsored by the Department of Homeland Security (DHS) Domestic Nuclear Detection Office (DNDO) and conducted by Sandia National Laboratory and the Southwest Research Institute looked at the specific vulnerabilities to devices commonly found in research and medical settings. These include blood and research irradiators which use Cs-137 and gamma knifes which use Co-60. These reviews improved our understanding of device vulnerability to theft or sabotage in the absence of any NRC security-increased controls or GTRI voluntary security enhancements.

The key finding of this study was that the radioactive sources within self-shielded cesium irradiators could be extracted more quickly than initially thought. GTRI, DNDO, and NRC agreed that adding additional hardening to cesium irradiators was prudent. This study led to the cesium chloride In-Device Delay (IDD) effort that will be described in section III.B below.

II.D Multiple Open Sites

Radiological sources are located at thousands of civilian sites across the United States and around the world. Medical, university, and research facilities are, by nature and design, "open" environments that allow a larger set of people access to these materials. These types of facilities are more difficult to secure than isolated military installations or nuclear power plants which are designed to be closed to all but a very limited number of personnel.

II.E Insider Threat

It is important to not focus solely on attacks from outside terrorists attempting to penetrate and steal material. GTRI also looked at threats from the insider, i.e., someone who works at a facility and likely has intimate knowledge of security procedures and vulnerabilities. The possibility and probability of a passive insider, e.g., one who simply arranges access to the facility for the adversary, or an active insider, one who participates in the theft, diversion, or sabotage of radiological material, is greater given the "open" environment of a university campus or city hospital in which many radiological devices are used.

III. GTRI'S ROLE IN MITIGATION OF RISKS

GTRI works very closely with its Federal partners, each of which has a unique role ensuring a comprehensive system of oversight, prevention, and protection of civilian radiological sources. DHS's mission is to prevent terrorist attacks within the United States; reduce the vulnerability of the United States to terrorism; and, minimize the damage, and assist in the recovery, from any terrorist attacks that do occur within the United States across multiple sectors (e.g. nuclear, chemical, etc.), leading the Government Coordinating Council(s) (GCC) and collaborating with the industry-led Sector Coordinating Council(s) (SCC) to protect critical infrastructure and key resources. NRC's mission is to license and regulate the Nation's civilian use of by-product, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment. The Federal Bureau of Investigation (FBI) is the lead Federal law enforcement agency and plays a significant role preventing, interdicting, and investigating potential acts of nuclear and radioactive theft, sabotage, or terrorism. NNSA brings the science and expertise of our National Laboratories to create innovative solutions to prevent the acquisition of nuclear and radiological materials for use in weapons of mass destruction (WMD) and other acts of terrorism. Specifically, GTRI and the DOE laboratories provide unique expertise to evaluate radiological issues and threats because of our significant work both internationally and domestically which allows us to identify "best practices" available in each circumstance.

To address the risks outlined above, GTRI, in cooperation with its Federal partners, has initiated a number of voluntary security efforts to further mitigate these potential threats. These include eliminating unwanted sources, hardening kits for specific irradiators, facility-wide voluntary security enhancements, specialized training courses for security and law enforcement personnel, and table top exercises for first responders. GTRI's voluntary security enhancements complement and do not replace NRC's increased controls requirements. When requested by the licensee, GTRI works to assess existing security conditions, provide recommendations on security enhancements, and when warranted, fund the procurement and installation

[3] *Radiation Source Use and Replacement,* National Academy of Sciences (February 20, 2008).

of jointly agreed-upon security best practices. GTRI considers all 14 isotopes of concern above threshold quantities (10 Ci or greater), and addresses several areas of security including Deterrence, Control, Detection, Delay, Response, and Sustainability.

GTRI's voluntary security enhancement efforts have been endorsed by the NRC, DHS, FBI, Organization of Agreement States (OAS), and Conference of Radiation Control Program Directors, Inc. (CRCPD). NRC has issued Regulatory Information Summaries (RIS) describing both the IDD and voluntary security enhancement efforts of GTRI and recommends that licensees volunteer for these GTRI efforts.[4]

III.A Elimination—Removing Unwanted Sources

Since 1997 GTRI's Off-Site Source Recovery Project (OSRP) operated by Los Alamos National Laboratory, Idaho National Laboratory and the CRCPD has reduced the radiological risk by recovering and eliminating disused and unwanted sealed sources. GTRI, in coordination with NRC, developed recovery prioritization criteria based on risk reduction. As of August 31, 2009, GTRI has recovered over 22,700 sources (totaling more than 720,000 curies) in 12 years.

At present, only 14 States in the United States have access to commercial disposal for sealed sources (with the exception of Ra-226 sources which have a commercial disposal pathway in all 50 States). With the decline in commercial disposal options, GTRI has seen an increase in the number of sources being registered as excess and unwanted. GTRI has found that without disposal access, source owners have no option other than long-term storage, which increases the vulnerability of becoming lost or forgotten.

III.B Delay—CsCl Irradiator In-Device Delay (IDD)

A fundamental component of GTRI's voluntary security enhancements is delay. By increasing delay (the amount of time needed by the adversary to gain access to the radioactive sources) we give more time for law enforcement to interrupt the adversary before they can steal the radioactive source. As a result of the GTRI/DNDO cesium irradiator vulnerability study, NNSA, DNDO, and NRC along with cesium irradiator manufacturers developed In-Device Delay (IDD) hardening kits for the most widely used models of CsCl blood and research irradiators. The IDD kits make it orders of magnitude more difficult for an adversary to illicitly access and steal the radiological source.

In cooperation with the three principal manufactures (Best Theratronics, LTD., JL Shepherd and Associates, Pharmalucence) and the NRC, GTRI, and DNDO developed these kits and in August 2008 launched a voluntary pilot program to install them. Some of the first sites to volunteer for the IDD kits included New York's Sloan-Kettering Institute for Cancer Research, Mt. Sinai School of Medicine, St. Vincent's Hospital and Medical Center, University of Pennsylvania, University of Rutgers, Wake Forest University, Baylor College of Medicine, University of Miami—Miller School of Medicine, and Geisinger Health System.

The installation of these kits is often carried out in extremely sensitive and very busy research and hospital environments. This requires the installers to use special measures (e.g. sound dampening, exhaust and fume hoods, etc.) and that coordinate installation schedules in order to minimize the impact on these facilities. Installations generally take 8 to 16 hours depending on the type of device, and are usually scheduled during evening hours to minimize the impact on research or medical operations. In May 2009, DNDO transferred their portion of the IDD project to GTRI in order to streamline the IDD effort and consolidate all relevant voluntary source security activities under one Federal agency (many licensees have irradiators from more than one manufacturer at their site). This transfer of scope has allowed GTRI to standardize processes and procedures across all three manufacturers, and ensures that the project is coordinated with other GTRI source security efforts. The pilot project has been deemed a success and GTRI has initiated a national rollout plan to outfit all qualifying irradiators in the United States.

The total number of cesium devices in the United States is about 1,100. Nearly 260 of these devices are small calibration units or self-contained irradiators located at nuclear power plants or other secure locations. The remaining 840 devices are self-contained irradiators located at universities, hospitals, and research institutes. Each one of these 840 CsCl irradiators has enough material that could be used in several RDDs of national significance.

---

[4] RIS 2008–17, July 18, 2008, "Voluntary Security Enhancements for Self-Contained Irradiators Containing Cesium Chloride Sources", and RIS 2008–23, October 3, 2008, "The Global Threat Reduction Initiative (GTRI) Domestic Threat Reduction Program & Federally Funded Voluntary Security Enhancements For High-Risk Radiological Material".

As of August 31, 2009 IDD kits have been installed on 32 irradiators. The remaining 808 irradiators can be hardened by fiscal year 2016. The implementation schedule is primarily constrained by human resource needs, scheduling complexities, and budget. Each manufacturer has a limited staff of trained employees that are approved to work on these devices. Locating, hiring, and training additional staff to supplement this effort is a lengthy process. Scheduling the installations is also a rate-limiting factor. Critical research schedules and blood bank operations cannot be disrupted. Simply finding a time when both manufacturer and facility can accommodate the installation adds time to the process. Each kit costs between $4,000–$8,000 in hardware and about $25,000 in installation labor and travel. The total estimated cost for 840 irradiators is $26 million. In addition, the manufacturers have agreed that starting in 2010 all new CsCl irradiators will have the IDD kits installed prior to sale and delivery.

In addition to the IDD hardening kits for CsCl irradiators, GTRI voluntary security enhancements also include other delay elements such as device tie-downs, locks, hardened doors/windows, walls, cages, and safes. All of these elements increase the time it takes the adversary to gain access to and steal the radioactive source.

III.C Detection—Remote Monitoring Systems (RMS)

A second fundamental component of GTRI's voluntary security enhancements is detection. Thirty minutes of delay with detection that allows responders to arrive in 20 minutes is considered to be effective. Thirty minutes of delay without detection that could allow the adversary to attack the source/device all weekend is considered to be not effective.

GTRI detection upgrades include biometric access control devices, door alarms, motion sensors, cameras, wireless electronic tamper indicating seals, and area radiation monitors. Each of these technologies provides a specific deterrence, control, and/or detection function that, when integrated together and with delay, provides a significant security enhancement in a holistic manner.

However, the most important feature of GTRI's detection enhancements is the remote monitoring system. This is because the remote monitoring system directly mitigates the two greatest vulnerabilities in securing an open civilian facility like a hospital or university: Which are (1) reliable transmission of alarms to the responders and (2) the insider threat.

Reliable transmission of alarms to the responders.—At military facilities and nuclear power plans, there are highly-trained operators who are located in hardened central alarm stations (CAS) who monitor the detection devices 24/7. These detection alarms are hardwired into the CAS and if an alarm goes off or the power is turned off, there is nearly 100 percent probability that the CAS operator will receive the alarm and immediately notify the large, well-trained, well-armed on-site response team as to the exact location and condition causing the alarm. In comparison, at many hospitals or universities, the alarms are not monitored by well-trained CAS operators sitting in a secure location. The alarms are instead sent to normal facility employees or unarmed guards on-site. Assuming the adversary hasn't already neutralized these lightly-armed on-site personnel, the emergency call will be handled by a 9–1–1 operator who will have little understanding of what an irradiator is or why cesium warrants an emergency response. The chances that a large, well-trained, well-armed off-site response will arrive in time from local law enforce under these conditions is greatly reduced due to the limited amount of reliable transmission of alarms.

Insider threat.—The greatest potential threat at hospitals and universities is that an insider could be the guard or employee who is on duty during off-hours an merely turns off or ignores the alarms. No one will know the source is gone until the next shift begins perhaps 12 hours or more later.

The GTRI remote monitoring system directly mitigates both of these threats by:

- Integrating alarms from multiple detection sensors and prioritizing alarms to ensure that critical alarms receive immediate attention even if the operator is not an expert in alarm assessment. The GTRI remote monitoring system includes statement of health and power level reports so external responders know immediately if the system is turned off.
- Alarms are simultaneously sent to multiple on-site and off-site locations such as ADT, local police departments, or regional fusion/operation centers. This ensures a timely response by sending a reliable transmission of alarms directly to trained off-site experts and responders. It also prevents against a single-point failure if the insider is the on-site alarm monitor or guard.

To address the sustainability portion of our security enhancement concept, GTRI provides a 3- to 5-year maintenance and warranty contract for each security enhancement device, contacts each site quarterly to follow-up on the status of the en-

hanced security system, and re-visits each site annually to determine if changes to the operating or threat environment warrant additional system enhancements.

GTRI prioritizes which sites receive voluntary security enhancements by assessing the attractiveness of the site's materials for possible use in an RDD, the site's proximity to DHS Urban Area Security Initiative (UASI) locations, and the site's proximity to other volunteer sites. GTRI estimates that there are about 2,200 buildings in the United States that house IAEA Category I or II levels of radiological materials. As of August 31, 2009, 37 buildings have been completed with the remaining buildings to be complete by fiscal year 2016.

GTRI also provide responders with radios, repeaters, and personal detection devices.

III.D Response—Alarm Response Training

The most important aspect of any security system is a timely, well-equipped, well-trained response team of appropriate size to interrupt and neutralize the adversary before they gain access to the radioactive source. GTRI has therefore made a focused effort to provide security personnel and local law enforcement with the tools and training needed to adequately respond to a security incident.

Most on-site guards at facilities with radioactive sources are not armed or large enough force strength to neutralize the threat. Therefore, the key responders are often off-site local law enforcement. Unfortunately, many local law enforcement officials are not made aware of the nature of the material which is in use at hospitals, blood banks, universities, oil fields, and manufacturing plants in their jurisdiction. It is important for their safety, and the safety of their communities, that they receive proper training about radiological sources. To ensure that both on-site and off-site responders understand how to respond to enhanced security system alarms, GTRI has developed an alarm response training course run by the Y–12 National Security Complex in Oak Ridge, TN.

This alarm response training prepares responders to protect themselves and the public when responding to events involving radiological materials. The participants conduct hands-on training in a realistic setting using actual protection equipment and real radioactive sources. The courses include operational exercise scenarios that build on classroom instructions and allow response forces to exercise their own procedures during realistic alarm scenarios.

As of August 31, 2009 we have conducted 6 training courses for 175 responders from 7 cities.

III.E Table Top Exercises (TTX)

As the capstone of GTRI's voluntary security enhancement support, GTRI has partnered with NNSA's Office of the Under Secretary for Counterterrorism and the FBI's Weapons of Mass Destruction Directorate to provide table top exercises at select nuclear and radiological sites. The purpose is to provide a no-fault, site-specific scenario where senior managers from various Federal, State, and municipal organizations can exercise their crisis management and consequence management skills in response to a terrorist incident. The overall objectives are:

- Promote cross-sector communication, cooperation, and team-building among Federal, State, local, and private sector first responders;
- Exercise FBI lead responsibility for criminal investigation;
- Examine newly developed tactics, techniques, and procedures resulting from GTRI voluntary security enhancements;
- Promote attack prevention through intelligence sharing and coordinated approach to neutralize the threat;
- Prepare site-specific integrated response plan with Federal, State, local, and private sector partners.

As of August 31, 2009 we have conducted 3 TTXs at facilities located in Honolulu, HI, Philadelphia, PA, and Manhattan, KS. A fourth TTX was recently completed in Houston, TX in early September.

III.F Transportation

Radioactive sealed sources may be at their most vulnerable when in transit. Recognizing this, GTRI has begun to implement security upgrades beyond regulatory requirements on our own source recovery shipments. GTRI has undertaken a number of pilot projects testing existing security devices/systems and has found that there is not a commercially available system that meets all our needs. Therefore, we are putting the best available compatible equipment on our vehicles and will continue to improve our system as additional technology advances are made. Because we are looking for a system(s) that private industry can adopt, we are working with the DHS-lead interagency group and directly with some in industry to demonstrate a prototype system using the best available devices. GTRI is offering indus-

try a test bed to evaluate their devices for compatibility and capability to operate in the harsh transit environment, (e.g., heat, cold, jarring, etc).

III.G Alternative Technologies

The ultimate risk reduction would be to replace radioactive sources with non-radioactive alternative technologies. NNSA's Office of Nonproliferation Research and Development is currently funding research into technologies such as is X-ray for blood irradiation, which uses electricity to create X-rays and cannot be used in a dirty bomb.

There have been recommendations to replace some radionuclides, particularly cesium chloride, with another form or radionuclide, e.g., cesium ceramic or cobalt. Caution must be given to ensure the new form will result in enough risk reduction to off-set the cost of developing the alternative and retrofitting/replacing current irradiators. GTRI is working with Sandia National Laboratories and Federal partners to perform a relative material risk reduction study to evaluate the amount of risk reduction that may be derived from an alternate form or alternate radionuclide to cesium chloride.

IV. COORDINATION AND COOPERATION

In implementing these voluntary security enhancements, GTRI has maintained close coordination and cooperation with Federal, State, and local agencies and the private sector. In particular, we have established strong working relationships with the NRC, DHS, and the FBI.

To coordinate these complementary efforts, GTRI participates regularly in meetings of the DHS-chaired Nuclear Sector Government Coordinating Council, the NRC-led Radiation Source Protection and Security Task Force, Tri-lateral meetings comprised of senior representatives from NNSA, DHS, and NRC, and many additional working level meetings. These coordination venues have helped ensure that officials throughout the Government are aware of new initiatives, on-going implementation efforts, and challenges encountered with enhancing radiological source security.

V. CONCLUSION

I am proud to report that GTRI, working in concert with our Federal, State, local, and private sector partners, has helped to further enhance security on radioactive sources and reduce the risk of a dirty bomb.

V.A Lessons Learned

Through our security efforts in the United States and overseas, we have learned several important lessons, paramount of which is that a well-trained, well-equipped, and timely response force is the single most important element in ensuring security. All the delay and detection in the world does not defeat the "bad guys"—the response team does. Since most non-power plant commercial sites do not have armed, 24-hour, on-site security personnel, it is the off-site local law enforcement that becomes the defacto 24/7 response to an incident of radiological theft or sabotage. Local law enforcement officers are not full-time radiological police, they have much broader duties to serve and protect the public, and they are not regulated by a Federal agency for radiological response effectiveness. It is for these reasons that GTRI has concentrated the vast majority of our voluntary security enhancements on helping these dedicated first responders. From our remote monitoring (which ensures they receive timely alarms and knowledge of the threat environment they will face) to personal protection equipment (radios and radiation pagers) to the realistic training and exercises. In addition, GTRI serves as a conduit to share lessons learned because we learn as much from local law enforcement as they learn from us. GTRI is able to share these lessons from site to site, city to city, and State to State to improve the collective security preparedness.

V.B Should Voluntary Efforts Be Mandated?

One of the most frequent questions we are asked is should these voluntary security enhancement be required? And if so when? These are very difficult questions to give specific answers to given the myriad of complex and interdependent risks that must be considered. For example:

- Which approach results in the faster implementation of effective security practices and risk reduction?
- How flexible will regulations be to take into account different industry sectors and the uniqueness of each site?
- How would you regulate local law enforcement or other off-site response team?

- What will be the cost burden imposed upon licensees and will it impact their ability to provide other critical services?
- How sustainable are voluntary upgrades that are not enforced through inspections?
- How do we encourage the licensees to ask security questions and push for best practices?

Our experience has shown that in most cases the fastest, most effective, and lasting way to improve security is to: (1) Fully engage the private sector, local law enforcement and the States in helping to create the appropriate security culture/program, and (2) by combining voluntary best practices to quickly and cost-effectively improve security at most sites and then follow that up in a few years with a new regulation to close the gaps.

In closing, Madame Chairwoman, thank you for inviting us to participate in today's important hearing. The Department of Energy has a dedicated team focused on reducing domestic and foreign radiological threats. GTRI's voluntary program has had an effective beginning, and we believe is well-positioned to bring about comprehensive solutions in a timely manner to the potential threat posed by radiological sources used in vital civilian applications.

Ms. CLARKE. Thank you very much.

Mr. Lewis.

STATEMENT OF ROBERT J. LEWIS, DIRECTOR, DIVISION OF MATERIALS SAFETY AND STATE AGREEMENTS (MSSA), NUCLEAR REGULATORY COMMISSION

Mr. LEWIS. Good morning. Madame Chairwoman, Members of the subcommittee, my name is Robert Lewis, and I am NRC's director of Materials Safety and State Agreements. I thank you on behalf of the Nuclear Regulatory Commission for holding this hearing on the important subject of securing radioactive sources. The NRC recognizes the direct role that radioactive source security plays in the agency's mission to protect public health, safety, and the environment.

On a personal level, I am a native New Yorker and a graduate of the SUNY system, so this venue I thank you for. It has particular significance to me.

I will now highlight some of the regulatory programs and recent accomplishments to tighten security of radioactive sources. My written testimony provides additional details.

The focus of Federal and State efforts to put in place tighter controls for security has been on radioactive sources that contain larger quantities, so-called Category 1 and 2 quantities, of key radionuclides of concern used in civilian applications across America, nuclides such as cobalt-60, cesium-137, iridium-192, and americium-241.

The civilian applications they are used for include food and medical equipment sterilization, medical research, cancer treatment, oil and gas exploration, and inspecting materials for hidden flaws during construction. Nation-wide, there are approximately 22,000 materials licensees, 1,300 of which possess Category 1 or 2 sources—approximately 1,300.

In conducting its mission, NRC partners with 36 Agreement States that regulate the possession and use of certain radioactive material within their States. Under these agreements, NRC relinquishes all of its regulatory authority over most radioactive materials in the State. However, we do work closely with the States to implement consistent and compatible National programs.

In addition, NRC oversees the Agreement State programs through periodic performance evaluations. New York is an Agreement State, and regulators for source licensing are the State health department and the New York City Department of Health and Mental Hygiene.

A key piece of legislation that has enabled regulatory enhancements on radioactive material security was the Energy Policy Act of 2005. Consistent with that law, NRC and Agreement States have employed a variety of tools to strengthen the U.S. systems for regulatory controls. I will use the rest of my time to highlight four of these: Increased controls in fingerprinting; cesium chloride studies; the National Source Tracking System; and enhanced interagency communications.

New security requirements, called increased controls, that were already mentioned have been issued in 2005 through 2006 by the NRC and the Agreement State regulators. Among other things, these require licensees to upgrade facilities and procedures to prevent and ensure detection of any unauthorized access to radioactive material. They also require advanced coordination with local law enforcement on security issues.

In 2007 to 2008, these controls were supplemented by requirements for fingerprinting and Federal criminal history background checks of anyone with unescorted access to Category 1 or 2 quantities of material. Licensees must establish and implement trustworthiness and reliability standards for such unescorted access.

A first round of increased controls inspections for compliance has been completed by NRC and all the Agreement States. The increased controls and fingerprinting requirements have been implemented for all Category 1 and 2 quantities of radioactive material, including approximately 550 licensees in the United States that possess about 1,100 self-contained cesium chloride irradiators. These are used to irradiate blood, conduct research, and calibrate emergency response radiation detection equipment.

They have long received—cesium chloride has long received increased attention from both a safety and security perspective because of its dispersible nature. Several studies, most recently and notably a 2008 National Academies report on source use and replacement, emphasize replacement technologies to be considered for cesium chloride, but also caution that any implementation consider preserving the essential functions of these devices.

NRC hosted a widely attended workshop in September 2008 to obtain input on the use and potential phaseout of cesium chloride. From this outreach and its own analysis, NRC concluded that near-term replacement of cesium chloride in existing blood research and calibration irradiators is not practicable and would disproportionately be detrimental to medical care, continuity of research, and the provisions for emergency response capability.

NRC believes it is imperative to develop a viable alternative technology and a disposal option for these sources before considering a phaseout. We are cooperating with the National Nuclear Security Administration program in which licensees voluntarily receive hardware improvements to the irradiators to enhance security beyond requirements.

The Energy Policy Act also included a provision for the National Source Tracking System, a Web-based database to ensure and enhance accountability of radioactive sources. Since it was deployed in January of this year, all transactions including Category 1 and 2 sources have been reported into the system, and over 55,000 sources are currently tracked. This greater accountability directly strengthens the national security framework.

Finally, I would like to mention that the level of interagency coordination on source security issues, from our perspective, has never been higher. This is the result of the Government-wide Radiation Source Protection and Security Task Force, established by the Energy Policy Act and chaired by the NRC; the Government coordinating councils that have been mentioned by DHS; and the trilateral meetings that have already been mentioned.

That concludes my prepared remarks. Thank you for the opportunity to testify today at this hearing, and I look forward to responding to your questions.

[The statement of Mr. Lewis follows:]

PREPARED STATEMENT OF ROBERT J. LEWIS

SEPTEMBER 14, 2009

Chairwoman Clarke, Members of the subcommittee, Members of the House from the New York City area, I am here today representing the Nuclear Regulatory Commission (NRC) staff to provide a status report that describes our approach to improving safety and security of radioactive sources and our recent accomplishments in this important area. Thank you for the opportunity to provide you with an overview of the Nation's regulatory programs to tighten security requirements for the highest risk radioactive sources.

BACKGROUND

To put the radioactive source security improvement efforts into context, it is important to first provide some background on the 2003 International Atomic Energy Agency (IAEA) Code of Conduct on the Safety and Security of Radioactive Sources, which Congress, in the Energy Policy Act of 2005, directed NRC to implement. The NRC's program to tighten security and controls on the highest risk radioactive sources is founded in and consistent with the United States Government's commitment to the Code of Conduct. The Code of Conduct identifies 16 radionuclides of concern, along with a categorization by radioactivity levels for each radionuclide, based upon the relative health hazards each radionuclide would present if not kept under adequate controls. Sources and devices containing Category 1 and 2 quantities of these materials are the most dangerous, and have been the focus of Federal and State efforts to put in place tighter controls for security. Of the 16 radionuclides, only four are widely used in civilian applications in this country: Cobalt-60, cesium-137, iridium-192, and americium-241. Civilian applications include food and medical equipment sterilization, medical research, cancer treatment, oil and gas exploration, and inspecting materials for hidden flaws.

NRC has been a world leader in applying the Code of Conduct through strengthening the U.S. system of regulatory controls, including: Imposing enhanced import/export controls in 2005; requiring users of the sources to upgrade their facilities, information controls, and control of personnel access to the radioactive sources since 2005; establishing and using an Interim Inventory of Nationally Tracked Sources since 2004, and upgrading the Interim Inventory via the deployment of the National Source Tracking System in 2009. In these initiatives, however, NRC coordinates in partnership with the 36 Agreement States that regulate the possession and use of certain radioactive material in their States pursuant to agreements between the NRC and the Governor of each State. These agreements are provided for by section 274 of the Atomic Energy Act, as amended. Under these agreements, NRC relinquishes its regulatory authority over radioactive materials in that State; NRC does retain responsibility for nuclear reactors, nuclear fuel cycle facilities, as well as for Federal facilities' material licensees, such as military and veterans hospitals. NRC and the Agreement States work very closely to implement consistent and compatible

programs for regulating radioactive materials safety and security across the country. In addition, NRC provides oversight of each Agreement State program through a periodic performance evaluation program. New York is an Agreement State, and the regulators are the State Health Department and the New York City Health Department.

Nation-wide, there are a total of 22,000 U.S. materials licenses. Of these, less than 10 percent (approximately 1,300 licensees) possess IAEA Category 1 or 2 sources. There are also an estimated 30,000 active general licenses that permit possession of smaller quantities of radioactive material in devices (e.g. industrial gauges), which do not require a specific license application or regulatory review process because of the inherent safety of the devices and resulting low risk of an accident.

A key piece of legislation that has enabled regulatory enhancements to radioactive materials security is the Energy Policy Act of 2005. This law included provisions that expanded NRC's fingerprinting and background check authority, required study of radiation source use and replacement, mandated the creation of a National source tracking system, and created an interagency Radiation Source Protection and Security Task Force. I will use the remainder of my statement to address the progress made and continuing work in each of these areas.

INCREASED CONTROLS AND FINGERPRINTING

The licensees that possess Category 1 or 2 materials as defined by the IAEA Code of Conduct have all had to comply with new requirements called "increased controls," which were issued in 2005–2006 by the NRC or Agreement State regulators. The increased controls have required licensees to upgrade their facilities and procedures to ensure detection and prevention of unauthorized access to radioactive material, advance coordination with local law enforcement, enhanced security during transportation, and enhanced and frequent accounting of sources. These measures also require licensees to establish and implement trustworthiness and reliability standards to determine who will have unescorted access to the radioactive material. Those that are not approved to have unescorted access must be within line of sight of an approved individual when accessing the material. NRC and Agreement States verify compliance through inspections of licensees. The first round of increased controls inspections for all licensees has been completed and compliance issues corrected.

From 2007–2008, the increased controls were supplemented by additional requirements for fingerprinting and Federal criminal history records checks of all individuals with unescorted access to Category 1 or 2 quantities of radioactive material to further improve the tools available to determine trustworthiness and reliability. The NRC and all of the Agreement States are now in the process of verifying compliance through the inspection process. Since December 2007, an estimated 90,000 fingerprint forms have been submitted and processed.

The NRC and Agreement States are jointly developing new materials security regulatory requirements that reflect the experience gained through implementation of the increased controls and fingerprinting requirements. Draft regulatory text was made available for public review on Regulations.gov and we expect a proposed rule to be published in the Federal Register for public comment by early 2010.

STRATEGY FOR THE SECURITY AND USE OF CESIUM CHLORIDE SOURCES

In 2006, the Radiation Source Protection and Security Task Force provided the President and Congress a report, as mandated by the Energy Policy Act of 2005. One of the key recommendations in the report focuses on the security of radioactive sources containing cesium chloride in a highly dispersible form. Since that time, there have been a number of recent Federal studies to assess options for the continued use of cesium chloride as the chemical form for radioactive cesium-137 sources. Cesium chloride is a salt that is sealed into a welded, doubly encapsulated stainless steel capsule, and used to irradiate blood and tissue, conduct bio-medical and materials science research, and calibrate emergency response radiation detection equipment. Cesium chloride has long received increased attention from both a safety and security perspective because of its potential dispersibility if removed from the irradiator and the source capsule, which could spread radioactivity. Approximately 550 licensees in the United States possess about 1,100 self-contained cesium chloride irradiators. These devices contain a Category 1 or 2 quantity of cesium-137 as defined by the IAEA Code of Conduct. The NRC's and Agreement States' increased controls and fingerprinting requirements have been implemented for all of these devices.

In February 2008, the National Academies issued a report on Source Use and Replacement that emphasized replacement technologies should be considered for cesium chloride because the National Academies considered this radioactive source a greater concern under certain attack scenarios than others based on its dispersibility, solubility, penetrating radiation, source activity, and presence in population centers across the country. In light of multiple views on alternative technologies and replacement, NRC convened a public workshop on September 29–30, 2008, to obtain input on the use and potential phase-out of cesium chloride. The workshop had 210 participants and we received 141 written comments after the workshop. We also asked NRC's Advisory Committee on Medical Uses of Isotopes (ACMUI) to complete a study comparing cesium chloride blood irradiation to other technologies, particularly X-ray irradiation.

In light of the various stakeholder comments, the ACMUI study, and its own analyses, NRC concluded that near-term replacement of cesium chloride sources or devices in existing blood, research, and calibration irradiators is not practicable and would be disproportionately detrimental to the delivery of medical care, the continuity of longstanding research, and the provision of emergency response capabilities. Therefore, NRC believes it is imperative to develop a viable alternative technology and a disposal option for these sources before considering a phase-out.

Research to develop an alternative chemical form for large activity cesium-137 sealed sources could provide a pathway to long-term phase-out of these sources in favor of those with diminished utility in a radiation dispersal device. While it is not the NRC's role to conduct such research, we are engaging our Federal partners in efforts to identify a lead agency or agencies to conduct research and/or to provide incentives to facilitate development of alternative chemical forms for cesium-137. Because all cesium-137 chloride is currently produced at one facility overseas and given the extensive use of irradiators outside of the United States, international engagement and cooperative efforts towards exploring new international standards for such sources are a necessary part of any long-term solution.

The NRC and Agreement States, along with the Department of Homeland Security's (DHS) Domestic Nuclear Detection Office, are working in close cooperation with the Department of Energy's National Nuclear Security Administration's (NNSA) voluntary program to install hardware improvements that are retrofitted to existing irradiators and incorporated into the designs of newly manufactured irradiators. These modifications to enhance security extend beyond current regulatory requirements. Also, these efforts are often complemented by expert security guidance to licensees (called assist visits) and table-top exercises with a view towards sharing best practices.

The NRC is continuing to work with Federal, State, and international partners to assess the risk environment and to encourage further technological developments for alternative forms of cesium-137. The increased controls required by the NRC and Agreement States and implemented by licensees, along with voluntary additional facility and device hardening measures, have significantly improved the security of these sources.

NATIONAL SOURCE TRACKING SYSTEM

NRC has maintained an Interim Inventory of Nationally Tracked Sources since 2004, which was an annual accounting of licensees authorized to possess Category 1 and 2 sources. The Energy Policy Act of 2005 included a provision for the National Source Tracking System (NSTS), which supersedes the interim inventory. The NSTS is a secure, Web-based database that is readily accessible to appropriate personnel and is designed to enhance the accountability for radioactive sources. The NSTS directly enhances the ability of the NRC and Agreement States to: (1) Verify legitimate ownership and use of nationally tracked sources; (2) conduct inspections and investigations; and (3) communicate information to other Government agencies. Since NSTS was deployed in January of this year, all transactions involving Category 1 or 2 sources, such as manufacture, transfer, and disassembly, have been required to be reported to this system. Over 55,000 sources are currently tracked in the system. This greater accountability for these sources helps strengthen the national security framework from initial production through final disposition of these sources.

The NSTS also directly demonstrates our leadership to other countries in applying the IAEA Code of Conduct by complying with its recommendations to have a national registry of radioactive sources. In the coming years, the NRC is planning to further improve the functionality of the NSTS. We will integrate NSTS data with Nation-wide licensing information to further enhance our capabilities to track compliance and authorize transfers of radioactive material.

INTERAGENCY COOPERATION AND COMPLEMENTARY EFFORTS ON RADIOACTIVE SOURCE SECURITY

The NRC has several major efforts underway with regard to U.S. interagency coordination.

The Government-wide Radiation Source Protection and Security Task Force, which was established by the Energy Policy Act of 2005, has been one of the primary vehicles for discussing and addressing issues relating to the security of radiation sources. This Task Force has senior representatives from 14 Federal and State agencies that have a role in radiation source security. In August 2006, the Task Force delivered a report to the President and to Congress that included 10 recommendations and 18 actions, addressing areas such as alternative technologies, cesium chloride, public communications, and the use of better tools to identify sources of concern. Progress has been made on each of these recommendations and actions. The next report is due to the President and Congress in August 2010, and will provide an integrated view of the various activities that have been completed within the last 4 years or are underway.

DHS is responsible for convening Government Coordinating Councils for critical infrastructure, including the nuclear sector. NRC routinely coordinates with, and provides updates of agency activities to, Federal partners through the Nuclear Government Coordinating Council. Both the Agreement States and the non-Agreement States also participate.

NRC also participates in periodic trilateral meetings with DHS and NNSA to coordinate source security activities. These trilateral meetings enhance coordination and awareness of each agency's activities and initiatives regarding source security.

The activities described above demonstrate that there is a coordinated U.S. Government approach to source security.

CONCLUSION

The NRC recognizes the direct role that radioactive source security plays in the agency's mission to protect public health, safety, and the environment. NRC and Agreement State requirements serve as a firm foundation for security that ensures that all licensees provide a common baseline level of security that is adequate to protect public health, safety, and the environment. The application of increased controls, the deployment of the National Source Tracking System, and the NRC's cooperative efforts across the Federal community have comprehensively and significantly improved the security of radioactive sources.

Thank you for the opportunity to testify today at this hearing. I look forward to responding to your questions.

Ms. CLARKE. Thank you, Mr. Lewis.

Captain Riggio, I would like to just ask your indulgence and the rest of the panel and my colleagues. You know, when you enter into someone's house, it is really important that they welcome you there. I neglected to have the chief executive officer, Debra Carey, greet us and would like to do so at this time.

So, Ms. Carey, would you please join us here?

Ms. CAREY. Good morning. Thank you, Madame Chairwoman.

So I just wanted to take a minute. You are already very much into a very, very important topic, in terms of the emerging threats, cybersecurity, and science and technology. It was kind of a test to see if I could remember the subcommittee.

But I would also like to welcome the Honorable Congressman Lungren, the Honorable Congresswoman Sanchez, and the Honorable Congresswoman Richardson. Welcome so much to Brooklyn. Definitely, we are so pleased to have you here at SUNY Downstate Medical Center.

I will not take but a second, really, because it is a very important topic here and I don't want to delay the subcommittee hearing any longer, but we are so pleased that you have chosen us to actually have the hearing here, because we are in a unique position because not only are we an educational institution, which many of you

know us as a college of medicine, but basically we are also a hospital, which is what I run. So, therefore, we are a user of radiological materials. We also clearly are responders. You have one of our outstanding members of our faculty and the leader of our disaster preparedness efforts here at the hospital and the campus, Dr. Arquilla, who is one of the witnesses. But, also, we have a special goal and mission of protecting the community.

So all of this is so relevant for us. What we want to thank you for is coming and making us a partner in this. Anything that we can do to facilitate and help, such as this, having hearings, even having other public hearings, we are more than happy to provide the location. So, again, thank you so much, and I hope it is a wonderful hearing.

Thank you.

Ms. CLARKE. Thank you, Ms. Carey. We appreciate your hospitality and lending us of your faculty and facilities here.

We are going to return now to our proceedings with Captain Riggio of the New York Police Department.

STATEMENT OF CAPTAIN MICHAEL RIGGIO, COUNTERTERRORISM DIVISION, NEW YORK POLICE DEPARTMENT

Mr. RIGGIO. Thank you, Madame Chairwoman, Ranking Member Lungren, Ms. Sanchez, Ms. Richardson. Good morning. Welcome to Brooklyn.

As the Chairwoman said, my name is Michael Riggio. I am the commanding officer of the NYPD's CBRNE—Chemical, Biological, Radiological, Nuclear and Explosives—Countermeasures Section. On behalf of Deputy Commissioner Richard Falkenrath, our commissioner for counterterrorism, I thank you, and I am grateful for this opportunity to speak with you this morning.

At the NYPD, as you probably know, we are proactively engaged in a multifaceted approach to combating terrorism; that being nuclear threats and radiological threats, as well. We dedicate a variety of resources to combating those, which include personnel, technology, training, and equipment. In speaking of terms that we are here for, we do a variety of things to combat the threat of an RDD and that of an IND as well.

The Counterterrorism Division began conducting radioactive/radiological source security assessments in 2003. Those efforts quickly progressed as we were preparing for the Republican National Convention here in the city in the summer of 2004.

The Department, the Counterterrorism Division, in cooperation with the New York City Department of Health, the NRC, and the Department of Energy, began conducting numerous security vulnerability assessments at several facilities here in New York City that contained high-consequence radioactive sources. These assessments revealed to us that a large amount of these sources were stored at medical facilities.

As a result of these assessments, recommendations were made to enhance the security posture at each of these facilities. After the Republican National Convention and as a result of the NRC's increased controls imposed on Agreement States in 2005, the Division began working with many of the city's medical and industrial facilities to work on hardening and securing.

Today, the Division, as a stand-alone unit and in partnership with the New York City Department of Health, we conduct vulnerability assessments and do security recommendations to approximately 100 facilities here in the city.

In the summer of 2006, NYPD began working with the Department of Homeland Security's Domestic Nuclear Detection Division on a multi-State program called Securing the Cities. As was mentioned earlier, the goal of the Securing the Cities program is to create an architectural framework, a foundation in and around New York City and this region to interdict an RDD or IND or the materials that are used to assemble such devices.

The NYPD has 12 principal partners in the Securing the Cities program, which represents over 150 law enforcement agencies across three States: New York, New Jersey, and Connecticut.

The Securing the Cities partners realize that, while New York City remains the top terrorist target, planning, preoperational surveillance, and bomb making will likely occur outside of New York City in these partners' jurisdictions. For this reason, the New York-area Securing the Cities program has greatly enhanced the detection and interdiction capabilities of the States of New York, New Jersey, and Connecticut by providing local law enforcement agencies with several thousand pieces of radiological interdiction/detection equipment, which is deployed in the tri-State area daily.

To do its part, we, the New York City Police Department, deploy over 1,000 radiological detection and interdiction assets on a daily basis. They are deployed by routine patrol officers, specialized patrol officers, and those on assignments in strategic locations. They include the use of checkpoints, chokepoints, mobile detection systems, handheld detection systems, and personal radiological detection systems.

Within the Securing the Cities program, there are six subcommittees that help run day-to-day operations, each of them with a specific measure of how do we interdict a radiological device.

One of those such subcommittees, the Source Security Subcommittee, is specifically dedicated to ensuring that facilities that use or store materials within the New York region are visited and surveyed. The goal is to ensure that source security is conducted regionally and that a consistent security posture exists within the region for all locations where radiological sources of concern are located.

Additionally, the NYPD ensures a high level of security for those radioactive sources that are moving through or within the city. Our Operations Division is tasked with making sure that we have uniformed personnel assigned to cover these deployments, which include vehicle escorts, plain-clothed and uniformed officers on the scene.

The NYPD conducts several counterterrorism deployments on a daily basis. These deployments all have a radiological interdiction component to them. They include critical response vehicles, Operation Hercules, Operation TORCH, and radiological chokepoints. These deployments consist of multiple vehicles on a daily basis, at least 75, that go to many of the city's critical locations.

In addition, the Operation Hercules and the Operation TORCH use ESU officers with heavy weapons and tactical gear, combined

with K–9 officers, to sensitive locations and transportation hubs. Many of the personnel involved in these deployments have personal radiation detection devices on them.

Additionally, we set up several radiological chokepoints daily throughout locations in the city for the purpose of choking traffic down to one lane and screening every vehicle that goes by.

Recently, an industrial radiograph which possessed a radioactive source was reported missing from an industrial radiography company located in one of the city's five boroughs. This type of device and others like it which are inside these facilities are used to inspect metals and light alloys for structural defects.

Members of the NYPD and the FBI conducted an investigation into the missing device. The device, which was ultimately found and returned, was found to be during the course of interviews that were conducted—it was claimed by some employees in this industry that these devices are often removed after-hours for personal matters.

While the NYPD at this point cannot confirm how widespread this practice is, it should be noted that the insider threat poses a great risk to the security of this industry. The NYPD is currently working with the New York State Department of Health to investigate this matter further and remedy it.

Finally, the NYPD supports any efforts to increase and toughen the NRC's regulation and oversight authority to ensure that every facility in this great Nation that handles radiological sources is as tightly monitored and secured as those here in New York City.

While we, the New York City Police Department, never take a moment off to prevent an attack here in New York City, we have no ability to prevent the theft of dangerous radiological and nuclear materials at facilities and locations that are outside of our control. We hope that the NYPD's efforts will serve as a model for other cities.

Members of the committee, I thank you for your time. I apologize; the red light has been on for a little while.

[The statement of Mr. Riggio follows:]

PREPARED STATEMENT OF MICHAEL RIGGIO

SEPTEMBER 14, 2009

Good morning Chairwoman Clarke, Ranking Member Lungren, and Members of the House Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. My name is Captain Michael Riggio, and I am the Commanding Officer of the NYPD Counterterrorism Bureau's Chemical, Biological, Radiological, and Nuclear Section. On behalf of Dr. Richard Falkenrath, the New York City Police Department's Deputy Commissioner of Counterterrorism, I am grateful for this opportunity to address you.

The NYPD is proactively engaged in a multi-faceted approach to protecting the city from terrorism, including radiological and nuclear terrorism. The NYPD has dedicated a variety of resources to combating the threat posed by radiological sources and radiological and nuclear weapons, including: Personnel, technology, equipment, and training. We are particularly concerned with two threats: Radiological dispersal devices (RDD), such as "dirty bombs", and improvised nuclear devices (IND).

BACKGROUND AND BEGINNINGS

The NYPD's Counterterrorism Division began conducting radiological source security assessments in 2003. Those efforts quickly progressed as the city prepared for the Republican National Convention in the summer of 2004. The NYPD, in partner-

ship with the New York City Department of Health and Mental Hygiene, the Department of Energy, and the Nuclear Regulatory Commission (NRC), conducted security vulnerability assessments of several facilities that contained high-consequence radioactive sources. These assessments revealed that large amounts of materials were stored in New York City hospitals and medical research facilities. Most of these sources were in moderately secure locations and were used for medical therapy (e.g., oncology, X-rays, and sterilization of blood supplies, etc.). As a result of these assessments, recommendations were made to enhance the security posture of each facility.

After the Republican National Convention, and as a result of the NRC's Increased Controls (IC) imposed on Agreement States in 2005, the Counterterrorism Division began working with many of the city's medical and industrial facilities that have radiological sources that meet the IC's quantity threshold. Today, the Counterterrorism Division, as a stand-alone unit and in partnership with the New York City Department of Health and Mental Hygiene, conducts site surveys and provides security recommendations to almost 100 facilities within the city of New York. These security recommendations include, among other things: Limiting access to rooms that contain equipment with radiological sources by requiring a personal code or key card; and monitoring access with CCTV cameras and other access-tracking technology.

SECURING THE CITIES

In the summer of 2006, the NYPD began working with the Department of Homeland Security's Domestic Nuclear Detection Office (DNDO) on a multi-state regional partnership called Securing the Cities. The goal of the Securing the Cities program is to create a layered architectural framework, or foundation, in and around the city of New York to detect and interdict an RDD, an IND, or the radiological materials needed to assemble such devices. The NYPD has 12 principle partners in this effort, representing over 150 agencies, in three States—New York, New Jersey, and Connecticut.

The Securing the Cities partners realize that while New York City remains a top target for terrorist groups, planning, pre-operational surveillance, and bomb-making may occur outside of the city, in partner jurisdictions.

For this reason, the New York Area Securing the Cities program has greatly enhanced the detection and interdiction capabilities of the States of New York, New Jersey, and Connecticut, providing local law enforcement agencies with thousands of pieces of radiological detection and interdiction equipment. This equipment is deployed daily by personnel in the tri-State area.

To do its part, the NYPD deploys over 1,000 radiological detection and interdiction assets on a daily basis. These assets are deployed by patrol officers performing routine duties, specialized duties, and those on assignment at strategic locations. We use checkpoints, chokepoints, mobile detection systems, and handheld detection.

Within the Securing the Cities program, there are six subcommittees that help run day-to-day operations, each of which oversees an important aspect of the radiological interdiction mission. The "Source Security Subcommittee" is specifically dedicated to ensuring that facilities that use or store radiological materials within the New York region are visited and surveyed. The goal is to ensure that source security is conducted regionally, and that a consistent security posture exists within the region for all locations where radiological sources of concern are located. This subcommittee is also preparing a best-practices document to ensure that consistent and easily identified standards are instituted and practiced within the region.

SOURCE MOVEMENT

Additionally, the NYPD ensures that a high level of security is maintained during the movement of sources of concern. The NYPD's Operations Division is notified any time a radiological source is being transported into or through New York City. The Operations Division coordinates the Department's response and patrol deployments during these transports. This may include vehicle escorts and uniformed and plainclothes on-scene security.

COUNTERTERRORISM STRATEGIC DEPLOYMENTS

The NYPD conducts several counterterrorism deployments on a daily basis. They include: Critical Response Vehicle (CRV) surges; Operation Hercules; Operation Transit Operational Response Canine Heavy Weapons (TORCH); and Radiological Chokepoints.

A CRV deployment consists of over 75 marked police cars on a single tour of duty that deploy to sensitive locations based on daily intelligence. This deployment is

highly flexible so that personnel can be redeployed during operations as events unfold locally and globally. The supervisors who oversee these deployments are all equipped with personal radiation detection devices.

Operation Hercules deploys Emergency Services Unit (ESU) officers with heavy weapons and tactical gear, canine officers, highway patrol officers, and detectives from the NYPD Intelligence Division, to sensitive locations throughout the city on a daily basis. Similarly, Operation TORCH deploys ESU officers with heavy weapons and tactical gear, canine officers, and a counterterrorism liaison officer, to the city's critical transportation hubs. Each of the ESU officers involved in these deployments is equipped with a personal radiation detector, and some are trained to use advanced radiation detection equipment.

Finally, radiological chokepoints are set up to interdict radiological sources at several locations throughout the city each day. At these chokepoints, uniformed personnel operate advanced detection vehicles and equipment. They also scan each vehicle that passes through a single lane of traffic at approximately 5 miles per hour. At all of these deployments, all alarms are investigated and resolved.

RECENTLY DISCOVERED VULNERABILITY

Recently, an industrial radiograph, which possessed a radioactive source, was reported missing from an industrial radiography company located in one of the city's five boroughs. This type of device is used to inspect metals and light alloys for structural defects. Members of the NYPD and the FBI's Joint Terrorism Task Force conducted an investigation into the missing device. The device was ultimately returned to the company. In the course of interviews conducted during the investigation, it was claimed that some employees in this industry remove these devices after hours.

While the NYPD cannot confirm how widespread this practice is, it should be noted that the insider threat presents a security risk to the industry. The NYPD is currently working with the New York State Department of Health to investigate this incident and to develop strategies that will help prevent this from happening again.

CONCLUSION

Finally, the New York City Police Department supports any efforts to increase and toughen the NRC's regulations and oversight authority to ensure that every facility in the United States that handles radioactive sources is as tightly monitored and secure as those in New York City. While we never stop working to prevent an attack within New York City, we have no ability to prevent the theft of dangerous radiological and nuclear materials at facilities and locations that are outside of our jurisdiction. We hope that the NYPD's efforts to secure radiological sources will serve as a model for other cities.

Members of the Committee on Homeland Security and the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, I thank you for your time this morning and I look forward to working with you to protect our country from radiological and nuclear threats. Thank you.

Ms. CLARKE. Thank you. You had a very compelling testimony. We appreciate that, Captain.

Mr. Miskin.

STATEMENT OF GENE MISKIN, DIRECTOR, OFFICE OF RADIOLOGICAL HEALTH, NEW YORK CITY DEPARTMENT OF HEALTH AND MENTAL HYGIENE

Mr. MISKIN. Thank you, Madame Chairwoman and distinguished Members of the committee. I am pleased to have this opportunity to discuss the efforts the New York City Department of Health and Mental Hygiene in conjunction with its Federal, State, and local partners have made to ensure the security of radioactive materials in the city.

As mentioned, New York State is an Agreement State, but it is unique in that there are three regulatory agencies in the State that are responsible for the agreement, one of which is the Department of Health and Mental Hygiene in the city.

The department's regulatory oversight of radioactive materials allows it to expand upon Federal security requirements and foster on-going working relationships among the regulative community, the NYPD, and other first-responder agencies. This collaboration could serve as a National model for how to approach radioactive material security.

The department has taken a comprehensive approach to improving security for both large and small quantities of radioactive material. We work cooperatively with the NYPD to address law enforcement aspects of security, along with the public health and safety issues involved.

The department also works with the regulative community, providing information on best practices for security by bringing in highly trained experts from outside of the regulatory environment. This approach takes general security requirements and makes them specific to individual licensed facilities.

I will highlight now the department's oversight of compliance with the Nuclear Regulatory Commission initiatives and our efforts to augment and support Federal regulatory framework.

We instituted the Increased Control Program in 2005 by issuing commissioner's orders to facilities that met the criteria for increased controls. We did our first round of IC inspections, completed by 2007, and currently are on our third round of IC inspections, almost completed.

For the fingerprinting requirement under section 652 of the Energy Policy Act, we informed our licensees, our IC licensees, that we would be making rulemaking and including that language in our health code for the city and gave them a heads-up, told them it was coming. By October 2008, the Board of Health had approved that language, and it is now sitting in our regulations.

In December 2008, we issued 39 license amendments to those facilities that had sources that fit reporting requirements for the National Source Tracking System.

So the department has had substantial and timely compliance with these Federal regulatory mandates dealing with security of radioactive materials, but we have developed several important local initiatives that support and augment these requirements.

Using Department of Homeland Security Urban Area Security Initiatives and CDCBT grants, plus using city tax levy funds, the department has developed and is in the testing phase of its New York City Radiation Data System, or NYCRADDS. The system serves as a single data repository for all activities dealing with ionizing radiation in the city. One part of NYCRADDS is an almost real-time inventory of all radioactive material located at our various licensees' facilities. Licensees report using a secure website and include radionuclides on hand, the activities of these radionuclides, and their specific location on-site.

In 2004, the department, with the assistance of the U.S. Department of Homeland Security, visited seven large licensees to assess security programs in place and then to make recommendations for security updates. The effort was well-received by our licensees and indicated the value of expanding these reviews to other licensees. The Department of Homeland Security then provided a grant to the department to widen the security assessment visits, and we con-

tracted with Brookhaven National Laboratory to support our efforts.

The review team itself was comprised of a department staff person, an NYPD officer from the counterterrorism bureau, a private security specialist, and a health physicist from Brookhaven. This project has provided detailed security assessments to 80 licensed facilities in the city. Twenty of these facilities included increased control facilities, and 60 that did not meet the IC radioactive requirements but had various amounts of radioactive material onsite.

All licensees received radioactive material security self-audit checklists, training materials for security staff, and guidance representing radioactive material security best practices. The department is working with Brookhaven to complete a written guidance document, "Best Practices for the Security of Radioactive Materials," and will distribute it to most of our 360 licensed facilities.

In 2007, the department conducted a training session for the radiation safety officers of our large facilities on the use of the NYCRADDS radioactive material inventory website. Testing of this system is almost complete, and the final training package is being prepared for the remainder of our licensees.

In 2008, the department participated in a pilot project sponsored by the Department of Homeland Security in which three of our hospital licensees had security enhancements made to their cesium-137 irradiators. On April 1, 2008, the department hosted a symposium entitled, "Radiation Security: Preventing Radioactive Materials from Getting Out and Preventing Radioactive Contamination from Getting In." There were 110 attendees, including radiation safety officers, security personnel, the NYPD, and FDNY.

In conclusion, the department has made and continues to make the security of all radioactive materials in the city a high priority. The regulatory and nonregulatory approaches we have taken have resulted in improved security at all of our licensed facilities and have reduced the probability, we feel, of domestic radiological threat from materials that are used in this city.

Again, thank you for the opportunity to let you know what we are doing, and I will be happy to answer your questions.

[The statement of Mr. Miskin follows:]

PREPARED STATEMENT OF GENE MISKIN

SEPTEMBER 14, 2009

I am pleased to have this opportunity to discuss the efforts the New York City Department of Health and Mental Hygiene (the department), in conjunction with its Federal, State, and local partner agencies, has made to ensure the security of radiological materials.

The department plays a unique role in regulating radiological sources. New York City is one of only a few cities that have direct regulatory oversight of nearly all radiological sources. New York State is an Agreement State, which means that the State and the United States Nuclear Regulatory Commission (NRC) have entered into an agreement under the former Atomic Energy Act to delegate authority to New York State (NYS) to regulate radioactive material at non-reactor sites within its jurisdiction. The New York State Agreement comprises three regulatory programs—administered by the New York State Department of Health, New York State Department of Environmental Conservation, and New York City Department of Health and Mental Hygiene. Under this structure, the department, through the Office of Radiological Health (ORH), regulates radioactive material for medical, research, and academic purposes within the five boroughs of the city. The depart-

ment's regulatory requirements for radioactive material are contained in Article 175 of the New York City Health Code.

The department has taken a comprehensive approach to improving security for both large and small quantities of radioactive materials. First, the department is responsible for regulating the public health and safety aspects related to the use of radioactive materials. This includes all non-exempt radioactive materials, not just materials in quantities of concern. Second, the department works cooperatively with the New York Police Department (NYPD) to address law enforcement aspects of security and public safety. Third, the department works cooperatively with the regulated community, providing information on best practices and facilitating access to highly-trained experts outside the regulatory environment.

The department's regulatory oversight of radiological materials allows it to expand upon Federal requirements and foster on-going working relationships among the regulated community, the NYPD, and other first responders; this collaboration could serve as a National model for how to approach radioactive materials security. While placing appropriate priority upon resources and efforts to secure the facilities with the highest-risk materials, New York City's approach has been to take a more expansive view of potential risks and provide multiple avenues to help the regulated community to understand the measures it can take to properly secure radioactive material.

In addition to inspecting the regulated communities for compliance with Federal standards, the department has developed new systems to track the location, quantities, and types of radiological materials located in New York City; provided local facilities with access to security experts to evaluate their security measures; and sponsored symposia and educational forums for the regulated community and first responders. By ensuring regulatory compliance as well as augmenting the best industry practices for physical security, we can reduce the risk of criminal activity involving any amount of radioactive material.

I will now highlight critical aspects of the department's oversight of compliance with NRC-required security initiatives and efforts to augment and support the Federal regulatory framework:

NRC REQUIRED SECURITY INITIATIVES

Increased Control

In 2005, the NRC required that Agreement States initiate the Increased Control (IC) requirements for their licensees that have certain radionuclides in quantities of concern. The department identified 32 facilities representing 47 licenses that met this criterion or could meet the criterion based on the limits on radiological materials in their licenses. On October 20, 2005, the department held a meeting to educate and inform its largest licensees about IC requirements. This meeting was also attended by the NYPD.

In December 2005, the department issued a Commissioner's Order to those licensees meeting the NRC's criterion to institute the Increased Controls (IC) by June of 2006. Since that time, the number of licensees subject to the IC requirements has been reduced to 20 facilities because some either legally disposed of radioactive materials or amended their licenses to reduce their possession limits for the radionuclides of concern.

In preparation for the expanded inspection of IC facilities, three department staff members attended an NRC-sponsored IC training in 2006. In compliance with NRC inspection mandates, the department inspected all of the facilities required to meet the IC requirements. These inspections, performed jointly with the NYPD Counter Terrorism Division, were completed by March 2007. The second round of joint IC inspections was completed by August 2008, and the NYPD also participated in these inspections. The third round of IC inspections is under way, and the department is well ahead of NRC time frames.

The department's inspections indicated that while all facilities inspected were in substantial compliance with the NRC's IC requirements, violations—either of rules and regulations or of security requirements in need of upgrading—were found in about 25 percent of inspected facilities.

Fingerprinting and Criminal History Check Requirements

The NRC also requires fingerprinting and criminal background checks for all individuals with unescorted access to radioactive materials in quantities of concern, under authority granted by Section 652 of the Energy Policy Act of 2005 (EPAct). Criminal histories obtained from the Federal Bureau of Investigation are used, along with other factors, to determine whether these individuals should continue to have such access. The NRC has imposed this fingerprinting requirement upon all

licensees who are subject to Increased Controls, including Agreement State Licensees. Background checks were to be completed by June 2, 2008.

On April 25, 2008 the department's Office of Radiological Health advised its IC licensees of this requirement, and that we would be initiating appropriate rule-making to include it in Article 175 of the New York City Health Code. In September, 2008, the NYC Board of Health approved the addition of the fingerprinting language to Article 175, and it became effective in October, 2008.

While the department's inspections have found that all facilities have made substantial progress toward compliance with the fingerprinting requirements, many facilities require improvement in documentation.

National Source Tracking System

NRC initially deployed the National Source Tracking System (NSTS) in December 2008 to track the deployment of Category 1 and 2 sealed sources from cradle to grave. Category 1 and 2 sealed sources are listed in 10 CFR 20 Appendix E. Agreement State licensees are required to use the system to report inventories of these sealed sources directly to NRC and to update the inventories as needed. The department issued 39 license amendments to licensees that possessed these categories of sealed sources, requiring them to use the NSTS for reporting purposes, between March and June 2009.

Overall, we find substantial compliance with Federal regulatory mandates, but we have developed several important local initiatives that support and augment the Federal regulatory framework, which I will now describe.

NEW YORK CITY DEPARTMENT OF HEALTH AND MENTAL HYGIENE SECURITY INITIATIVES

The department has initiated a series of efforts that support and augment the Federal regulatory framework for ensuring the security of radioactive materials, as briefly described at the opening of my statement. I will highlight several of these efforts.

NYCRADDS

Using Federal grant monies from the Center for Disease Control and Prevention and city tax levy funds, the department is developing the New York City Radiation Data System (NYCRADDS). The system serves as a single repository of all licensing, permitting, inspectional activity and radioactive materials inventory in New York City. Included in NYCRADDS is the ability for a facility, through a secure website, to report radionuclides on hand, their activities, and specific on-site locations of the material. Facilities are requested to make quarterly reports so that it is a near real-time inventory of radioactive material in New York City that can be shared with our partner local, State, and Federal agencies as needed.

Grant-funded Security Reviews of New York City Hospitals

In 2004, with the assistance of the U.S. Department of Homeland Security (DHS), the department visited seven IC facilities in New York City, and made recommendations for security upgrades to the licensees. The results of these visits indicated the value of expanding these reviews to other licensees. DHS provided a grant to the department to widen the security assessment visits and we contracted with Brookhaven National Laboratory to support our efforts. A security review team consisting of a staff person from the department, an NYPD officer from the Counter Terrorism Bureau, a private security specialist, and a health physicist from Brookhaven National Laboratory, visited licensed facilities. This project provided detailed security assessments to 80 facilities, including 20 licenses that are required to comply with the Increased Controls. In addition to the on-site consultations performed, licensees were also given a Radioactive Materials Self Audit Checklist to use for self audits, training materials for security staff, and written guidance representing radioactive materials security best practices. The department is presently working with Brookhaven National Laboratory to complete a written guidance document *Best Practices for the Security of Radioactive Materials,* and will distribute this guidance to all or most of the approximately 360 licensed facilities in New York City.

DOHMH Sponsored Meetings and Symposia

In September 2007, the department conducted a training session for the radiation safety officers of our larger facilities on use of the NYCRADDS Radioactive Materials Inventory website. Testing of this system is almost complete, and a final training package is being prepared for the remainder of our licensees.

In 2008, the department participated in a pilot project sponsored by DHS in which three of our hospital licensees had security enhancements made to their Cesium-137 irradiators.

On April 1, 2008, the department hosted a symposium entitled "Radiation Security: Preventing Radioactive Materials from Getting Out and Preventing Radioactive Contamination from Getting In." There were 110 attendees, including radiation safety officers, security personnel, NYPD, and FDNY. The purpose of the symposium, funded by the DHS Urban Areas Security Initiative, was twofold: (1) To reiterate the security requirements for those institutions subject to the U.S. Nuclear Regulatory Commission's Increased Controls Program; and, (2) to provide an update and highlight best practices of a department grant-funded program that provided participating hospitals with area monitors capable of detecting radioactively-contaminated persons entering their facilities. NYPD's Counter Terrorism Bureau discussed protocols to be followed in the event of equipment alarms going off. The department plans to pursue additional Federal funding for future programs dealing with security and detection of radioactive materials in the city.

Non-regulatory Approaches To Augment Federal Regulatory Efforts

The department has initiated non-regulatory reviews of security efforts at IC and non-IC facilities, providing facilities with access to a team made up of a regulator, a physical security expert, an NYPD officer, and a specialist in radiation protection. This effort has provided direct assistance and educational materials to foster the development of best practices among facilities managing smaller quantities of radiological materials of concern, such as research labs that are not required to meet enhanced Federal security mandates. The department believes that the incorporation of non-IC facilities into its security efforts is critically important to ensure the security of radioactive materials in New York City.

By conducting these visits outside the regulatory process, the department gained voluntary access to these facilities, and could facilitate improvements at many IC and non-IC facilities in New York City. These detailed on-site evaluations employed a graded approach to security for these materials, which helped facilities identify typically inexpensive physical security upgrades and/or changes to administrative procedures. For example, the department has developed a best practices manual that provides easy-to-follow security check-lists, which facilities can use to evaluate their own security measures and to self-identify enhancements.

The department has emphasized reducing vulnerabilities by increasing controls and administrative improvements, such as improved access control, background checks, enhanced material control and accountability, coordination with local law enforcement agencies, proper display of picture identification badges, background checks for unescorted access to materials, key control and accountability, and discontinued dual use of space for radioactive sources. The department's approach has resulted in documented improvements in controls, and has had a positive influence on facilities with both high-activity and low-activity radioactive sources.

In conclusion, the department believes that its strategic vision, employing an asystematic approach, has reduced the probability of domestic radiological threat from materials used in New York City.

Thank you for the opportunity to testify on the department's radioactive materials security initiatives. I will be pleased to answer any questions you may have.

Ms. CLARKE. Thank you, Mr. Miskin.

Dr. Arquilla.

STATEMENT OF BONNIE ARQUILLA, DIRECTOR OF DISASTER PREPAREDNESS, SUNY DOWNSTATE MEDICAL CENTER

Dr. ARQUILLA. I would like to thank the committee for inviting me to speak. My background is in emergency medicine, with an emphasis on disaster preparedness at SUNY Downstate Medical Center. We have created a number of guidelines and full-scale exercise drills to examine disaster preparedness. As an emergency medicine physician, I do clinical work at University Hospital-Brooklyn and Kings County Medical Center.

The two hospital facilities I mentioned on Clarkson Avenue see the majority of patients in central Brooklyn. We have a special research interest in vulnerable populations, such as pediatrics and

geriatrics. Obviously, my primary viewpoint is around the preparations that hospitals can make to provide better care for the neighborhoods they serve in addition to hospital care of the sick or injured.

We are also acutely aware that we are the safety net for disaster relief in central Brooklyn and New York City. So what would happen if there were a dirty bomb, a nuclear explosion or covert release of radiological material? Database and exercises we at SUNY have conducted in collaboration with other organizations tell us that we are not adequately prepared to respond to the expected overwhelming influx of patients seeking medical evaluation and assurances. However, it must be noted that most of these patients would not be at immediate medical risk.

For the purposes of this testimony I have been asked to address the following issues: A basic review of radiation; a few scenarios where the population might be exposed to radiation; acute medical issues around radiation exposure; the response framework established at SUNY, while identifying important gaps; and the necessity of securing potential radiation sources.

For the interest of time, although I submitted it in writing, the basic review of radiation I will skip at this time.

Scenarios where the population might be exposed to radiation: While most us are familiar with dirty bombs, another type of attack, the "I-cubed"—for ingestion, inhalation, and immersion—these attacks are not accompanied with a flash and bang.

Fortunately, it is hard to kill a lot of people with an ingestion attack. Contaminating a reservoir or even a water main is ineffective because radioactivity is quickly diluted. However, the population knowing that an attempt has been made may be enough to create a disaster. This is an important issue that should have Government attention. Training and education and risk communication must be better to help our population better cope with their fears.

An inhalation attack, sometimes called a smoky bomb, uses radioisotopes that can be burned, vaporized, or aerosolized in a confined space to contaminate the air. The subway, for example, is an ideal location. The population inhales the contaminated air, with the effect of either killing quickly by radiation poisoning or slowly by causing cancer.

Obviously, this type of event detection is an area of importance, but it is not enough simply to detect and measure; we need a health care workforce that is trained to manage this type of exposure. I refer to Dr. Steven Becker's work. He shows a lack of understanding by many emergency department physicians of radiologic events and effects.

An immersion attack, or radioactive spray of hazardous material, is also very dangerous, because people wipe their faces and transfer the isotope to their mouth.

In a dirty bomb attack, health care workers are more concerned about the actual explosion rather than the radioactive effects of the blast. Blast injuries themselves kill more people and cause greater morbidity than the release of a nuclear agent.

Delays brought about by the need for screening of a hysterical population seeking to see if they are okay can wreak havoc on the system. Look at last spring with the flu. Many people presented for

evaluation to either their private physician's offices or hospitals just wanted to be sure that they either had the swine flu or not. Under regular circumstances, they would not have sought medical attention, and especially not emergency care. The hospitals in New York City were overwhelmed with ambulatory patients seeking reassurances.

The most important indicator of exposure of a patient is the time of onset of symptoms following irradiation. Vomiting within 2 to 4 hours is an indication of high-dose radiation. This is an emergency consideration. The greatest potential morbidity can be determined by the symptoms, where the patient was, the time of onset of symptoms, the point or source of contamination, what is the isotope—alpha, beta, or gamma—and length of exposure, external, and/or internal contamination.

The initial symptoms of acute radiation sickness include redness of skin, nausea, vomiting, and depressed white blood cell count. These are the effects we worry about predominantly for first responders and in major accidents with very high levels of radiation.

The prodromal phase is the phase after exposure to radiation with several vague, nonspecific symptoms. The latent phase: Patients appear asymptomatic typically for 2 to 4 weeks; then patients begin to develop infections. Usually, they require prophylactic antibiotics, antiviral, or antifungal agents. The illness phase is expressed by the damage to the specific organ system and depends on the level of whole-body exposure received by the patient.

Other effects of dirty bombs include traumatic injuries. This is thought to be a bigger killer in the short-term. The associated trauma that accompanies a dirty bomb attack presents the greatest risk to our emergency departments. Prolonged mental health problems are also an issue: Fear and panic, demand for medical resources, post-traumatic stress disorder, and stigmatization of those who are exposed. Often, these mental health after-effects of an event go untreated. This is a critical area for the Government to provide aid, focusing on first aid, mental first aid, screening, and long-term treatment.

The response framework established at SUNY Downstate: Preventing unnecessary exposure is the best defense, as my esteemed colleagues have already described. This is achieved also after the event by personal protective equipment such as gloves, over-garments, and respirators. Additional important safety measures include time, limiting the time of exposure; distance, maintaining a distance from the radioactive sources, which in our case would be contaminated patients or their clothing; and shielding, the use of PPE. Patients should be screened, stripped of all clothes that may hold radiation, showered, and rescreened.

Let me bring to your attention that I am not aware of any hospital that has a fully trained decontamination team in place, available 24 hours a day, 7 days a week. This type of specialized work is beyond the scope of the average health care worker. Currently, most decontamination teams are made up of volunteers, yet most health care workers are afraid to volunteer because they lack training.

Ideally, what is needed to rectify this situation is: Education of radiologic events and practices for health care workers; decon-

tamination training for health care workers, staff, and professionals, and with regular practice and recertification—many of our health care workers were trained 4, 5, 6 years ago and have not had retraining since then; Government support of the above, which includes funding.

Facility preparation and planning. I only have a second more. Important areas every facility should really look at is, where should the screening be done? Who should do the screening? Who needs to be screened? Noninjured, injured, and dead, personnel working in and around the event. Where should the radiation screening be done? The emergency department, the operating room, the decontamination area, the dressout areas, and any other area where contamination might occur. Radiation screening should also be done for personal belongings of victims, medical instruments, equipment, and waste.

Ms. CLARKE. Dr. Arquilla, can you summarize at this point?

Dr. ARQUILLA. Yes, that is why I turned the 3 pages. Thanks. Sorry.

In conclusion, National Opinion Research shows from the University of Chicago that, if a dirty bomb goes off, 65 percent of an urban population will self-evacuate without being informed to do so by the Government. They plan on going to emergency departments. This is 25 times the amount that we normally see, and we are already at 100 percent of our capacity.

As I mentioned earlier, risk communication training would be very important. Disaster preparedness training for emergency responders, emergency departments, and hospitals are also of vital importance.

Thank you. I am sorry I went over.

[The statement of Dr. Arquilla follows:]

PREPARED STATEMENT OF BONNIE ARQUILLA

ASSESSMENT OF PREPAREDNESS IN THE EVENT OF A RADIOACTIVE DISASTER

I would like to thank the committee for inviting me to speak. My background is in Emergency Medicine with an emphasis in Disaster Preparedness at SUNY Downstate Medical Center. We have created a number of guidelines and full-scale exercise drills to examine disaster preparedness. As an Emergency Medicine physician, I do clinical work at University Hospital, Brooklyn and Kings County Hospital Center. I have been the Director of Emergency Preparedness for both institutions since 2001. When I took over this post, it was chiefly a "regulatory position" to help the hospitals with JOINT commission inspections. With the September 11 and the anthrax terrorists attacks, that all changed.

Globally, we saw a critical need for preparedness. Medical professionals went about changing the culture of their hospitals; indeed all institutions and organizations address the need for a higher level of preparedness. It takes a generation to change cultural attitudes and so far, with regard to disaster preparedness, we've made good progress, but as with any ambitious goal or cultural shift, there's still more work to be done.

The two hospital facilities I mentioned earlier on Clarkson Avenue, see a majority of the patients in central Brooklyn. We have a special research interest in vulnerable populations such as pediatrics and geriatrics. Obviously, my primary viewpoint is around the preparations that hospitals can make to provide better care for the neighborhoods they serve, in addition to hospital care of the sick or injured. We are also acutely aware that we are the safety net for disaster relief in central Brooklyn and New York City . . . So what would happen if there were a dirty bomb, a nuclear explosion, or covert release of radioactive material?

Data based on exercises that we at SUNY have conducted in collaboration with other organizations, tells us that we are not adequately prepared to respond to the expected overwhelming influx of patients seeking medical evaluation and assur-

ances. However, it must be noted that most of these patients would not be at immediate medical risk!

For the purposes of this testimony I've been asked to address the following issues and concerns:

- A basic review radiation;
- A few scenarios where populations might be exposed to radiation;
- Acute medical issues around radiation exposure;
- The response framework established at SUNY, while identifying important gaps;
- The necessity to secure potential radiation resources.

A BASIC REVIEW OF RADIATION

The following are types of non-ionizing, harmless, radiation: Microwaves; Radio waves; Infra-red rays; Laser.

For the purposes of this inquiry, let's take a closer look at Ionizing Radiation.

What Is Ionizing Radiation? It is the spontaneous emission of "fragments" or "bundles" of energy from unstable nuclei creating more stable nuclei.

Ionizing radiation can rip off electrons from other atoms. It then attacks the atoms in living cells creating free radicals that damage our DNA. This is how it damages our cells. "The Cell/DNA itself is directly ionized by the radiation." This attack causes genetic mutation and the cells die from necrosis.

Following are Forms of Ionizing Radiation: Alpha particles; Beta particles; Gamma photons or gamma rays.

Alpha Particles are made up of two protons and two neutrons.

It's a helium nucleus, only with lots of kinetic energy. They are positively charged, physically large on the atomic scale—the heaviest and most highly charged.

Alpha Particles can normally be stopped by the dead layer of skin on the body or a sheet of paper.

Beta Particles are high-speed electrons stripped free from their atomic parent and sent off with kinetic energy. They are smaller and travel much faster than Alpha Particles. They may be positively or negatively charged.

Beta Particles can be stopped by 1 cm of plastic, wood, or paper. Like Alpha Particles, Beta Particles can cause damage to skin and other cells.

However, beta particles are not typically involved in acute radiological events.

Gamma Rays are packets of energy in the form of Photons, much like the visible light in this room, forming Electromagnetic Radiation (EMR) of high energy. Their interaction with materials is energy dependent. They can travel up to 1 mile in open air.

Gamma Rays are very penetrating and can pass right through the body. They are stopped best with lead or concrete. In high concentrations, they can penetrate to the bones and marrow and depress production of red blood cells. This is usually the type of radiation of most concern in disasters.

SCENARIOS WHERE POPULATIONS MIGHT BE EXPOSED TO RADIATION

While most of us are familiar with dirty bombs, another type of attack is the I-cubed (for ingestion, inhalation and emersion) these attacks are not accompanied with a flash and bang. Fortunately, it is hard to kill a lot of people with an ingestion attack. Contaminating a reservoir or even a water main is ineffective because the radioactivity is quickly diluted. However, the population knowing that the attempt has been made may be enough to create a disaster. This is an important area that should have Government attention. Training and education in "risk communication" must be better, to help our population better cope with their fears.

An inhalation attack, sometimes called a smoky bob, uses radioisotopes that can be burned, vaporized, or aerosolized in a confined space to contaminate the air. The subway, for example, is an ideal location. The population inhales the contaminated air, the effect either killing quickly by radiation poisoning, or slowly by causing cancer. Obviously, in this type of event detection is an area of importance, but it is not enough to simply detect and measure, we need a health care workforce that is trained to manage this type of exposure. Refer to Dr. Steve Becker's work. He shows a lack of understanding by many emergency department physicians of radiological events and effects.

An immersion attack, or radioactive spray, is hazardous because people wipe their face and then transfer isotope to the mouth.

In a Dirty Bomb attack health workers are more concerned about the actual explosion, rather that the radioactive effects of the blast. Blast injuries themselves will kill more people and cause greater morbidity than the release of the nuclear agent. Delays brought about by the need for screening of a hysterical population,

seeking to know if they are OKAY, and wreak havoc on the system! Look at last spring with the flu, many people who presented for evaluation to either private physician's offices or hospitals, just wanted to be sure that they had swine flu or did not. Under regular circumstances, they would not have sought medical attention and especially not emergency care. The hospitals in New York City were overwhelmed with ambulatory patents seeing reassurances.

ACUTE MEDICAL ISSUES AROUND RADIATION EXPOSURE

The most likely radioactive materials to be used in a terrorist attack are cobalt, strontium, cesium, and americium. All are poorly protected and readily available in medical, military, research, and industrial resources.

Cobalt is used in food irradiators and americium in used in smoke detectors and oil exploration.

Emergency Considerations

THE MOST IMPORTANT INDICATOR TO EXPOSURE OF A PATIENT IS THE TIME OF ONSET OF VOMITING FOLLOWING IRRADIATION. Vomiting within 2 to 4 hours is an indication of a high dose of radiation.

The greatest potential morbidity can be determined by:

- Symptoms?
- What are they?
- Time of onset?
- Point Source or Contamination?
- What is the isotope (alpha, beta, or gamma)?
- Length of exposure?
- External and/or internal contamination?

The initial symptoms to Acute Radiation Sickness include; skin redness, nausea, vomiting, and depressed white blood cell counts. These are the effects we worry about predominantly for first responders and in major accidents with very high levels of radiation.

The Prodromal Phase, is the phase after exposure to radiation with several vague, nonspecific symptoms.

In the Latent Phase patients appear asymptomatic typically for 2 to 4 weeks. Then patients begin to develop infections, usually require prophylactic antibiotics, antiviral agents, or antifungal agents.

The Illness Phase is expressed by damage to the specific organ system and depends on the level of "whole body" exposure received by the patient.

Other effects of Dirty Bombs include Traumatic injuries. This is thought to be a bigger killer in the short term. The associated trauma that accompanies a Dirty Bomb attack, presents the greatest risk.

Prolonged mental health problems:

- Fear/Panic;
- Demand for medical resources;
- Post Traumatic Stress Disorder;
- Stigmatization.

Often these mental "after effects" of an event go untreated. This is a critical area for the Government to provide aide, focusing on first aid, screening, and long-term treatment.

THE RESPONSE FRAMEWORK ESTABLISHED AT SUNY

Preventing unnecessary exposure is the best defense! This is achieved through Personal Protective Equipment (PPE) such as:

- Gloves;
- Over garments;
- Respirators.

Additional important safety measures include:

- Time—limiting the time of exposure;
- Distance—maintaining a distance from radioactive sources;
- Shielding—the use of PPE.

Patients should be screened, stripped of all clothes (they hold radiation), showered, and re-screened.

Let me bring to your attention, that I am not aware of any hospital that has a fully trained decontamination team in place and available 24 hours per day, 7 days per week. This type of specialized work is beyond the scope of the average health care worker. Currently, most decontamination teams are made up of volunteers. Yet, most health care workers are afraid to volunteer, because they lack training! Ideally, what is needed to rectify this situation is:

- Education—of radiological events and practices for health care workers;
- Decontamination training for health care staff and professionals as a regular part of their job;
- Government support of the above, including funding.

Facility Preparation & Planning

Important questions every facility should ask when responding are:

Who should get radiation screening?

- Patients that require monitoring and or admission to hospital.
- Non-injured, injured, dead.
- Personnel working in and around the event.

Where should radiation screening be done?

- ED, OR, decontamination area, dress out areas.
- Any other area where contamination might occur.

What other radiation screening should be done?

- Personal belongings of victims.
- Medical instruments, equipment.
- Waste.

How should radiation screening be handled? Or, what is the hospital's disaster procedure?

- Who will do screening?
- How will screening be done?
- How much equipment/PPE is needed to fulfill this mission?

Additional planning considerations:

- Pressure on normal ER staff;
- Press coverage;
- Psychological reaction of patients, public, and hospital staff;
- Prioritize areas, facilities, and equipment to be recovered:
  - What is needed ASAP?
  - What can wait?
- Establish a checklist for recovery.

THE NECESSITY TO SECURE POTENTIAL RADIATION RESOURCES

Once radioactive materials are no longer needed and the costs of appropriate disposal are high, security measures become lax, and the likelihood of abandonment or theft increases. We need to allocate funds for the safe disposal and storage of our radioactive materials.

In conclusion, the National Opinion Research Center at the University of Chicago reports that, "In the event of a dirty bomb explosion 65 percent of urban residents expect that they would evacuate after learning from the media that a dirty bomb has exploded, but without receiving any directive or information regarding the event from local government officials." Alarmingly, current guidelines say that people who received more that 25 times the threshold dose for evacuation would have to be taken into medical supervision. This would be an overwhelming number of people to evaluate and then follow for at least 25 years.

As I mentioned earlier, most medical facilities are simply not equipped to handle the large influx of "potential" patients who require reassurances. Our best defense against the effects of an I-cubed attack is to inform and educate the populace regarding their risk as soon after the attack as possible. Additionally, medical personnel and facilities should be prepared to deal with the specifics of such an attack. Currently, they are not. This can only be achieved through disaster preparedness training, the need for which cannot be overemphasized. It is my hope that the Homeland Security committee considers disaster preparedness training as part of their defense strategy in managing our country's safety against terrorists' attacks.

Thank you.

Ms. CLARKE. Thank you.

Mr. Aloise from GAO.

STATEMENT OF GENE ALOISE, DIRECTOR, NATIONAL RESOURCES AND ENVIRONMENT, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. ALOISE. Gene Aloise from GAO. Thank you, Madame Chairwoman.

Madame Chairwoman, Ranking Member Lungren, and Members of the subcommittee, we are pleased to be here today to discuss

how well-prepared we are as a Nation to recover from attacks using dirty bombs or an improvised nuclear device, otherwise known as an IND.

A terrorist's use of a dirty bomb or IND could have devastating consequences. Responding to such attacks is different than recovering from them. Response would include immediate actions as evacuations and providing medical treatment. Recovery includes cleaning up radioactive contamination from an attack so that people can return to their homes and businesses. Importantly, being prepared to recover from these attacks may even provide an element of deterrence if an adversary perceives less potential for lasting harm.

My remarks today will focus on Federal planning and clean-up capabilities and suggestions to improve our ability to recover from an attack. I will also discuss the United Kingdom's handling of the 2006 polonium incident and how that event has helped the United Kingdom better prepare for an attack.

Our work shows that most cities and States would be so overwhelmed by a dirty bomb or IND attack that they would rely on the Federal Government to conduct almost all clean-up activities that are an essential first step to recovery.

FEMA is responsible for developing a system to respond to and recover from terrorist attacks. However, planning by FEMA and other Federal agencies for recovering from such attacks is lacking. FEMA has not issued a national disaster recovery plan for dirty bomb or IND attacks. Also, existing Federal guidance provides little direction for agencies to develop their own recovery activities and test how well-prepared they are to implement recovery efforts. In fact, out of the 70 dirty bomb and IND exercises conducted over the last 5 years, only three have included a recovery component.

Regarding clean-up of radiation-contaminated areas, although research is under way, not much is known about how available technologies could be applied to an attack. The lack of guidance for identifying cost-effective clean-up methods in the event of an attack might mean that the clean-up approach taken could increase recovery costs. Experience has shown that using the wrong approach can generate waste types more difficult to remove than the original material.

In addition, limitations in testing thousands of material samples during clean-up after an attack and uncertainty about where to dispose of radioactive waste could also slow recovery. About two-thirds of the city, State, and Federal officials we surveyed expressed concern about the capability to provide the necessary clean-up actions to recover from an attack.

Furthermore, nearly all the cities and States we surveyed stated the need for a national disaster recovery strategy to address gaps in Federal guidance. Additional Federal guidance is needed in such areas as monitoring radiation levels, clean-up standards, and management of radioactive waste. In addition, most cities and States wanted more interaction with Federal agencies to test recovery preparedness.

Cities and States also expressed the need for intelligence information on dirty bomb and IND threats. They said that sharing information with law enforcement agencies is vital to planning. Only

about one-half of the officials from States considered at risk of an attack felt that they were getting sufficient intel information.

As part of our work, we also met with U.K. officials to discuss their handling of the 2006 polonium incident resulting from the murder of Alexander Litvinenko. While more limited in scope than what is envisioned by a dirty bomb, it had many of the characteristics of such an attack. Specifically, 47 sites across London had to be checked for radiological contamination, and about 20 were contaminated. Nine hundred people might have been exposed, and 20 showed signs of contamination, some significant. All of this from a gram of polonium-210 the size of a grain of salt.

According to U.K. officials, this incident proved the value of recovery planning. In particular, through this incident, U.K. officials gained an appreciation for the need to have an established clean-up plan, including a process for determining clean-up levels, sufficient laboratory capacity to analyze large quantities of samples for radiation, and procedures for handling radioactive debris. Furthermore, they found that the action taken as a result of this incident and other actions they have taken has better prepared the United Kingdom for dirty bomb or IND attacks.

Madame Chairwoman, that concludes my remarks. I would be happy to address any questions you may have.

[The statement of Mr. Aloise follows:]

PREPARED STATEMENT OF GENE ALOISE

SEPTEMBER 14, 2009

GAO HIGHLIGHTS

Highlights of GAO–09–996T, a testimony to Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

A terrorist's use of a radiological dispersal device (RDD) or improvised nuclear device (IND) to release radioactive materials into the environment could have devastating consequences. The timely clean-up of contaminated areas, however, could speed the restoration of normal operations, thus reducing the adverse consequences from an incident.

This testimony examines: (1) The extent to which Federal agencies are planning to fulfill their responsibilities to assist cities and their States in cleaning up areas contaminated with radioactive materials from RDD and IND incidents; (2) what is known about the Federal Government's capability to effectively clean up areas contaminated with radioactive materials from RDD and IND incidents, and (3) suggestions from Government emergency management officials on ways to improve Federal preparedness to provide assistance to recover from RDD and IND incidents. We also discuss recovery activities in the United Kingdom. This testimony is based on our on-going review of recovery preparedness issues for which we examined applicable Federal laws and guidance; interviewed officials from the Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Department of Energy (DOE), and Environmental Protection Agency (EPA); and surveyed emergency management officials from 13 large cities and their States, as well as FEMA and EPA regional office officials.

COMBATING NUCLEAR TERRORISM.—PRELIMINARY OBSERVATIONS ON PREPAREDNESS TO RECOVER FROM POSSIBLE ATTACKS USING RADIOLOGICAL OR NUCLEAR MATERIALS

What GAO Found

DHS, through FEMA, is responsible for developing a comprehensive emergency management system to respond to and recover from natural disasters and terrorists attacks, including RDD and IND attacks. The response phase would involve evacuations and providing medical treatment to those who were injured; the recovery

phase would include cleaning up the radioactive contamination from an attack in order to permit people to return to their homes and businesses. To date, much Federal attention has been given to developing a response framework, with less attention to recovery. Our survey found that almost all cities and States would be so overwhelmed by an RDD or IND incident that they would rely on the Federal Government to conduct almost all analysis and clean-up activities that are essential first steps towards recovery. However, we found that the Federal Government has not sufficiently planned to undertake these activities. For example, FEMA has not issued a national disaster recovery strategy or plans for RDD and IND incidents as required by law. Existing Federal guidance provides only limited direction for Federal agencies to develop their own recovery plans and conduct exercises to test preparedness. Out of over 70 RDD and IND exercises conducted in the last 5 years, only three have included interagency recovery discussions following a response exercise.

Although DOE and EPA have experience in the clean-up of small-scale radiation-contaminated areas, their lack of knowledge and capability to apply approaches to address the magnitude of an RDD or an IND incident could increase recovery costs and delay completion. According to an expert at Idaho National Laboratory, experience has shown that not selecting the appropriate decontamination technologies can generate waste types that are more difficult to remove than the original material and can create more debris requiring disposal-leading to increased costs. Limitations in laboratory capacity to rapidly test thousands of material samples during clean-up, and uncertainty regarding where to dispose of radioactive debris could also slow the recovery process. At least two-thirds of the city, State, and Federal respondents expressed concern about Federal capability to provide the necessary analysis and clean-up actions to promote recovery after these incidents.

Nearly all survey respondents had suggestions to improve Federal recovery preparedness for RDD and IND incidents. For example, almost all the cities and States identified the need for a national disaster recovery strategy to address gaps and overlaps in Federal guidance. All but three cities wanted additional guidance, for example, on monitoring radioactivity levels, clean-up standards, and management of radioactive waste. Most cities wanted more interaction with Federal agencies and joint exercising to test recovery preparedness. Finally, our review of the United Kingdom's preparedness to recover from radiological terrorism showed that that country has already taken actions similar to those suggested by our survey respondents, such as issuing national recovery guidance, conducting a full-scale recovery exercise, and publishing a national handbook for radiation incidents.

Madame Chairwoman and Members of the subcommittee: I am pleased to be here today to discuss preliminary observations from our on-going work reviewing the Federal Government's preparedness to assist localities in recovering from a terrorist attack involving either a radiological dispersal device (RDD)—frequently referred to as a dirty bomb—or an improvised nuclear device (IND). Responding to such an attack would involve evacuations, providing medical treatment to those who were injured, and protecting property; recovery would include cleaning up the radioactive contamination from an attack in order to permit people to return to their homes and businesses.[1] A terrorist's use of an RDD or IND to release radioactive materials into the environment could have devastating consequences. However, quickly analyzing and cleaning up contaminated areas after a deliberate release of radioactive materials could speed the recovery from such an attack by restoring normal operations of critical infrastructure, services, businesses, and public activities, and thus reducing the many adverse consequences from an attack. According to a recent report of the National Science and Technology Council, which coordinates science and technology policy within the Executive Office of the President, the ability of Government to quickly and decisively respond to and recover from an RDD or IND incident is key to national resiliency.[2] Importantly, the Council noted that being prepared to recover from these incidents may even provide an element of deterrence if the adversary perceives less potential for long-lasting harm.

The consequences of a terrorist attack using an RDD or IND would not only include loss of life but also enormous psychological and economic impacts. An RDD would disperse radioactive materials into the environment through a conventional explosive or through other means. Depending on the type of RDD, the area contami-

---

[1] For the purpose of this testimony, analysis activities include efforts to sample and analyze affected areas to determine the type and location of contamination, and clean-up activities include efforts to contain radioactive materials, decontaminate affected areas, and manage the radioactive waste.

[2] National Science and Technology Council, *Roadmap for Nuclear Defense Research and Development: Fiscal Years 2010–2014* (Washington, DC: July 2008).

nated could be as small as part of a building or city block or as large as several square miles. An IND would create a nuclear explosion producing extreme heat, powerful shockwaves, and intense radiation that would be immediately lethal to individuals within miles of the explosion, as well as radioactive fallout over thousands of square miles. Thus, the consequences of RDD and IND incidents would vary in magnitude, with an RDD expected to cause few deaths but produce significant economic and psychological impacts, and an IND causing thousands of deaths and more extensive destruction. An RDD is thought to be a more likely terrorist weapon than an IND given the prevalent commercial use of radioactive source material—for example, in some medical and industrial equipment—and the relatively uncomplicated way in which this material could be dispersed. In contrast, detonating an IND would require a terrorist group to obtain nuclear weapons material—which is generally heavily secured—and have highly sophisticated expertise and equipment to fabricate this material into a weapon.

If an RDD or IND incident occurred, a number of Federal, State, and local government departments and agencies would be involved in the analysis and clean-up of areas contaminated with radioactive material as part of the recovery process.[3] Generally, State and local governments have primary responsibility for recovering from disasters, but the Federal Government may provide assistance when an incident exceeds State and local resources or when an incident is managed by Federal agencies under their own authorities. The Department of Homeland Security (DHS) is the principal Federal agency for domestic incident management. The primary mission of its Federal Emergency Management Agency (FEMA) is to develop a comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation. For an RDD or IND incident, DHS would be the lead agency in coordinating Federal assistance to State and local governments. For these incidents, DHS would rely on other Federal agencies that have more experience with the analysis and cleanup of areas contaminated with radioactive materials. For example, in certain circumstances, the Department of Energy (DOE) would have primary responsibilities for the initial analysis of areas contaminated with radioactive materials, and the Environmental Protection Agency (EPA) would have primary responsibility for cleaning up the radiation-contaminated areas.[4] The Department of Defense (DOD) would act in support of the primary Federal agencies. Federal agencies, including EPA, DOE, the Nuclear Regulatory Commission, as well as State regulatory agencies have set various clean-up standards for decontaminating affected areas.

The risk of terrorists using an RDD or IND is, in large part, determined by their ability to gain access to the materials needed to construct these devices. Over the past few years, we have issued a number of reports on the security of nuclear and radiological materials, and facilities that house them. Overall, our work has shown that despite investing billions of dollars in new technology to upgrade security procedures, gaps continue to exist in our Nation's ability to prevent terrorists from accessing or smuggling dangerous quantities of radioactive material into the country. For example, in 2007, we testified before Congress that our own investigators were able to set up phony businesses and obtain a legitimate NRC license that would have permitted us to obtain dangerous quantities of radioactive material.[5] Our investigators were able to obtain this NRC license just months after NRC had completed a lengthy process to strengthen its licensing procedures. In 2008, we reported that NRC, in developing its security requirements for research reactors, had not fully considered the risks associated with terrorists attacking these facilities—many of which are located on college campuses.[6] Such an attack could involve terrorists sabotaging a reactor in order to disperse radioactive material over neighboring com-

---

[3] The Robert T. Stafford Disaster Relief and Emergency Assistance Act primarily establishes the programs and processes for the Federal Government to provide major disaster and emergency assistance to State and local governments, as well as to Tribal nations, individuals, and qualified non-profit organizations. Pub. L. No. 100–107, 102 Stat. 4689 (1988) (codified as amended at 42 U.S.C. § 5121 et. seq.).

[4] The Federal Radiological Monitoring and Assessment Center (FRMAC) is a DOE-led interagency asset that is available on request to respond to an RDD or IND incident. The FRMAC is responsible for coordinating all environmental radiological monitoring, sampling, and assessment activities for the response. DOE leads the FRMAC for the initial response phase and EPA assumes leadership for the clean-up phase.

[5] GAO, *Nuclear Security: Actions Taken by NRC to Strengthen Its Licensing Process for Sealed Radioactive Sources Are Not Effective,* GAO–07–1038T (Washington, DC: July 12, 2007).

[6] GAO, *Nuclear Security: Action May be Needed to Reassess the Security of NRC-Licensed Research Reactors,* GAO–08–403 (Washington, DC: Jan. 31, 2008).

munities—similar to an RDD. We have also reported on DHS's and FEMA's preparedness for, response to, and recovery from disasters in 2007, 2008, and 2009.[7]

Our testimony today presents preliminary observations from our on-going effort to examine: (1) The extent to which Federal agencies are planning to fulfill their responsibilities to assist cities and their States in cleaning up areas contaminated with radioactive material from RDD and IND incidents; (2) what is known about the Federal Government's capability to effectively clean up areas contaminated with radioactive material from RDD and IND incidents; and (3) suggestions from Government emergency management officials on ways to improve Federal preparedness to assist State and local governments in recovering from RDD and IND incidents. In addition, we are providing information on our review of actions taken in the United Kingdom to prepare for recovering from RDD and IND incidents. We expect to issue our final report on this topic in November 2009.

To address these objectives, we examined pertinent Federal law, Presidential directives, and other executive guidance; interviewed cognizant officials from DHS, DOE, EPA, FEMA, NRC, and National laboratories; and conducted a survey of emergency management officials in 13 cities considered to be at high or medium risk of such attacks, officials in these cities' States, and similar officials in all Federal FEMA and EPA regional offices.[8] We also reviewed information on the number and type of RDD and IND response and recovery exercises that have been conducted in the last 5 years. Finally, we visited the United Kingdom to review its preparedness to recover from RDD and IND incidents at the suggestion of EPA officials and because it has addressed a fairly recent radiological release incident in a large urban area.

BACKGROUND

In the aftermath of September 11, 2001, there is heightened concern that terrorists may try to smuggle nuclear or radiological materials into the United States. These materials could be used to produce either an IND or an RDD. An IND is a crude nuclear bomb made with highly enriched uranium or plutonium. Nonproliferation experts estimate that a successful IND could have a yield in the 10 to 20 kiloton range (the equivalent to 10,000 to 20,000 tons of TNT). An IND with a 20-kiloton yield would have the same force as the equivalent of the yield of the bomb that destroyed Nagasaki; it could devastate the heart of a medium-sized U.S. city and result in thousands of casualties and radiation contamination over a wide area.

Security experts have also raised concerns that terrorists could obtain radioactive material used in medicine, research, agriculture, and industry to construct an RDD, or dirty bomb. This radioactive material is encapsulated, or sealed in metal, such as stainless steel, titanium, or platinum, to prevent its dispersal and is commonly called a sealed radioactive source. These sealed sources are used throughout the United States and other countries in equipment designed to, among other things, diagnose and treat illnesses, preserve food, detect flaws in pipeline welds, and determine the moisture content of soil. Depending on their use, sealed sources contain different types of radioactive material, such as strontium-90, cobalt-60, cesium-137, plutonium-238, and plutonium-239. If these sealed sources fell into the hands of terrorists, they could use them to produce a simple, but potentially dangerous weapon, by packaging explosives, such as dynamite, with the radioactive material, which would be dispersed when the bomb went off. Depending on its type, amount, and form (powder or solid), the dispersed radioactive material could cause radiation sickness in people nearby and produce serious economic costs and the psychological and social disruption associated with the evacuation and subsequent clean-up of the contaminated area. While no terrorists have detonated a dirty bomb in a city, Chechen separatists placed a canister containing cesium-137 in a Moscow park in the mid-1990s. Although the device was not detonated and no radioactive material was dispersed, the incident demonstrated that terrorists have the capability and willingness to use radiological materials as weapons of terrorism.

---

[7] GAO, *Observations on DHS and FEMA Efforts to Prepare for and Respond to Major and Catastrophic Disasters and Address Related Recommendations and Legislation,* GAO–07–1143T (Washington, DC: July 31, 2007); *Actions Taken to Implement the Post-Katrina Emergency Management Reform Act of 2006,* GAO–09–59R (Washington, DC: Nov. 21, 2008); and *National Preparedness: FEMA Has Made Progress, but Needs to Complete and Integrate Planning, Exercise, and Assessment Efforts,* GAO–09–369 (Washington, DC: Apr. 30, 2009).

[8] The high- and medium-risk cities are Boston, Chicago, Dallas, Denver, Detroit, Houston, Los Angeles, Miami, New York, Philadelphia, San Francisco, Seattle, and St. Louis. While Washington, DC, is considered a high-risk city, we excluded it from our survey because it is unlike other cities in its reliance on the Federal Government and the Federal agencies that would take over analysis and clean-up activities.

Another form of nuclear terrorism occurred with the release of radioactive materials in London. In November 2006, Alexander Litvinenko, a former officer of the Russian Federal Security Service, was poisoned with a gram of polonium-210—about the size of a grain of salt.[9] His poisoning was detected only after he was hospitalized for a few weeks and tested for symptoms of radiation exposure because of hair loss. Following the poisoning, forensic investigators identified, with the help of the victim, 47 sites across London where he had been during the few days between his poisoning and death. Of these locations, about 20 showed signs of this radioactive material. Investigators identified over 900 people who might have been exposed to the polonium, including some who may have been exposed while aboard airplanes. After a thorough examination, a few of these individuals turned out to have significant exposure levels. The decontamination activities at these sites, including a hotel room, spanned 19 days, involved a number of methods and technologies, and cost in excess of $200,000.

CITIES AND STATES WOULD LIKELY REQUEST FEDERAL ASSISTANCE FOR CLEAN-UP OF RADIATION-CONTAMINATED AREAS AFTER RDD AND IND INCIDENTS, BUT LIMITED FEDERAL PLANNING EXISTS FOR RECOVERING FROM SUCH INCIDENTS

While State and local government responders would be expected to respond first to a terrorist incident within their jurisdiction, they would also expect that the Federal Government would be prepared to provide the necessary assistance for them to expedite the recovery from such an incident. Emergency management officials from 13 cities and the majority of their respective States indicated in our survey that they would rely on the Federal Government to conduct and fund all or almost all analysis and clean-up activities associated with recovering from an RDD or IND incident of the magnitude described in the National Planning Scenarios.[10] However, when asked which Federal agencies they would turn to for this assistance, city and State respondents replied inconsistently and frequently listed several Federal agencies for the same activity. In our view, these responses indicate that there is confusion among city and State officials regarding Federal responsibilities for these activities in the event of a terrorist incident. This confusion, if not addressed, could hamper the timely recovery from an RDD or IND incident. Emergency management officials from all the cities and most of their respective States told us they would rely on the Federal Government because their technical and financial resources would be overwhelmed by a large RDD incident—and certainly by an IND incident. Most of these officials believe they could adequately address a smaller RDD incident, such as one that is confined to a city block or inside a building.

Despite this anticipated reliance on the Federal Government, we obtained mixed responses as to whether these RDD and IND recovery activities should be primarily a Federal responsibility. Fewer than half of the respondents from the cities (6 of 13), but most of those from States (8 of 10) indicated that it should be primarily a Federal responsibility. The others stressed the need for shared responsibilities with the Federal Government. Despite the anticipated reliance by city and State governments on the Federal Government for analysis and clean-up activities following an RDD or IND incident, FEMA has not developed a National disaster recovery strategy or related plans to guide involvement of Federal agencies in these recovery activities, as directed by Federal law and executive guidance.[11] To date, much Federal attention has been given to developing a response framework, with less attention to recovery. The new FEMA coordinator for the development of a National disaster recovery strategy told us that while the previous administration had drafted a "white paper" addressing this strategy, the new administration has decided to rethink the entire approach.[12] She also told us that FEMA recognizes its responsibility to prepare a National disaster recovery strategy but she could not pro-

[9] Investigators believe that this pure polonium was probably produced in a Russian research reactor.

[10] The National Preparedness Guidelines (Sept. 2007) developed 15 national planning scenarios, including scenarios for RDD and IND incidents. The scenarios form the basis for coordinated Federal planning, training, exercises, and grant investments to prepare for emergencies of all types.

[11] The Post-Katrina Emergency Management Reform Act requires FEMA to report back to the Congress within 270 days of enactment of this 2006 legislation describing the details of a national disaster recovery strategy. Pub. L. No. 109–295, § 682, 120 Stat. 1355, 1445–46 (2006). In addition, the National Security Council, *National Strategy for Homeland Security* (Washington, DC, Oct. 2007), states that the Federal Government will prepare a framework for recovery.

[12] In our November 21, 2008 report (GAO–09–59R), we found that FEMA had drafted a national disaster recovery strategy but that it was under review at the time with no time frame for completion.

vide a time frame for its completion. However, she stated that when a recovery strategy is issued it should provide guidance to revise State, local, and other Federal agency operational plans to fulfill their respective responsibilities. Moreover, the FEMA official in charge of planning told us that the agency has put on hold issuing component plans that describe how Federal capabilities would be integrated to support State and local planning for response to and recovery from RDD and IND incidents.

Some existing Federal guidance documents addressing the assets and responsibilities of Federal agencies for both response and to a lesser extent recovery-related activities have been issued as annexes to the National Response Framework and in other documents.[13] For example, there is a nuclear and radiological incident annex, which describes the policies, situations, concept of operations, and responsibilities of the Federal departments and agencies for the immediate response and short-term recovery from incidents involving the release of radiological materials. There are also emergency support function annexes that provide a structure for coordinating Federal interagency support in response to domestic incidents.

In addition, two other sources of guidance have been issued that, according to FEMA officials, represent stop-gap measures until it can issue more integrated planning guidance. In 2008, FEMA issued updated guidance for protection and recovery following RDD and IND incidents.[14] This guidance was to provide some direction to Federal, State, and local emergency response officials in developing operational plans and response protocols for protection of emergency workers after such an incident. In regard to recovery, this document recommended a process to involve the affected public, State and local officials, and other important stakeholders in the identification of acceptable clean-up criteria, given the specifics of the incident. The other document, issued by the Homeland Security Council, pertains to responding to an IND in the first few days prior to the arrival of other necessary Federal resources. This document was prepared because the prior FEMA guidance did not sufficiently prepare State and local emergency response authorities for managing the catastrophic consequences of a nuclear detonation.[15] Moreover, DOE, EPA and DOD are developing more detailed operational guidance on their own based on the existing Federal guidance. For example, DOE has supported research on operational guidelines for implementation of protective actions described in the FEMA guidance,[16] EPA has drafted guidance for the optimization process following RDD and IND incidents,[17] and DOD has established operational plans for consequence management following terrorist incidents, including RDD and IND attacks.[18]

Federal agencies and local jurisdictions have been using the available guidance as a basis for planning RDD and IND exercises to test the adequacy of their plans and skills in a real-time, realistic environment to evaluate their level of preparedness. We identified more than 70 RDD and IND response exercises planned and carried out by Federal, State, and local agencies since mid-2003. However, officials with FEMA's National Exercise Directorate told us that only three of the RDD response exercises had a recovery component. According to these officials, recovery discussions following an RDD or IND response exercise have typically not occurred because of the time needed to fully address the response objectives of the exercise, which are seen as a higher priority. The most recent response exercise, based in Albany, New York, and planned by DOE, set aside 2 days for Federal, State, and local agencies to discuss operational recovery issues. One unresolved operational issue discussed during this exercise pertained to the transition of the leadership of the Federal Radiological Monitoring and Assessment Center (FRMAC) from the initial analysis of the contaminated area, led by DOE, to the later clean-up phase, led by EPA. For example, there are remaining questions regarding the level and quality

---

[13] DHS, *National Response Framework* (Washington, DC, Jan. 2008). This document provides a guide for how the Nation should conduct all-hazards response, including the roles and responsibilities of agencies involved in response efforts. It does not address long-term recovery issues, including cleaning up areas contaminated with radioactive materials.

[14] DHS, *Planning Guidance for Protection and Recovery Following Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) Incidents,* 73 Fed. Reg. 45,029 (Aug. 1, 2008).

[15] Homeland Security Council, *Planning Guidance for Response to a Nuclear Detonation* (Washington, DC: Jan. 16, 2009).

[16] C. Yu, et al. *Preliminary Report on Operational Guidelines Developed for Use in Emergency Preparedness and Response to a Radiological Dispersal Device Incident,* DOE/HS–0001 (Washington, DC: DOE, Office of Health Safety, and Security, February 2009). This document does not represent official policy, methods, or agency guidance.

[17] EPA, *EPA Guidance on the Optimization Process Following a Radiological Dispersal Device or Improvised Nuclear Device Incident* (Washington, DC: September 2009 Draft).

[18] We provided testimony on this DOD initiative in GAO, *Homeland Defense: Preliminary Observations on Defense Chemical, Biological, Radiological, Nuclear, and High-Explosive Consequence Management Plans and Preparedness,* GAO–09–927T (Washington, DC: July 28, 2009).

of the monitoring data necessary for EPA to accept the leadership of FRMAC. While we were told that this transitional issue has been discussed in exercises dating back to the development of the Federal Radiological Emergency Response Plan in 1984, it has only recently been discussed in RDD or IND response exercises. Another unresolved operational recovery issue pertains to the distribution of responsibilities for the ownership, removal, and disposal of radioactive debris from an RDD or IND incident. Both of these operational issues are to be examined again in the first full-scale RDD recovery exercise, planned and led by EPA, to take place April 2010.

INSUFFICIENT KNOWLEDGE AND CAPABILITY TO USE AVAILABLE APPROACHES FOR CLEAN-UP OF RADIATION-CONTAMINATED AREAS COULD IMPEDE EFFORTS TO RECOVER FROM RDD AND IND INCIDENTS

Although some Federal agencies, such as DOE and EPA, have substantial experience using various clean-up methods and technologies to address radiation-contaminated areas, little is known about how these approaches might be applied in an RDD or IND incident. For example, DOE has invested hundreds of millions of dollars in research, development, and testing of methods and technologies for cleaning up and decommissioning contaminated structures and soils—legacies of the Cold War. In addition, since the passage of the Comprehensive Environmental Response, Compensation, and Liability Act in 1980, which established the Superfund program, EPA has undertaken significant efforts to study, develop, and use technologies that can address radioactive contamination. DOD has also played a major role in studying potential applications for innovative technologies for its Superfund sites.

Not much is known, however, about the application to RDD and IND incidents of available clean-up methods and technologies because such an incident has never occurred in this country, although research is currently underway to gain a better understanding of potential applications. According to decontamination experts at Lawrence Livermore National Laboratory, current research has focused on predicting the effects of radiation release in urban settings through simulation, small-scale testing, and theory. In addition, researchers at EPA's National Homeland Security Research Center informed us that while there are standard methods and technologies for cleaning up radiation-contaminated areas, more research is needed to develop standard National guidance for their application in urban environments. The lack of guidance for identifying cost-effective clean-up methods and technologies in the event of an RDD or IND incident might mean that the clean-up approach taken could unnecessarily increase the cost of recovery. According to a decontamination expert at Idaho National Laboratory, for example, experience has shown that not selecting the appropriate decontamination technologies can generate waste types that are more difficult to remove than the original material and can create more debris requiring disposal—leading to increased costs. Moreover, he told us that without guidance and discussion early in the response phase, a contractor might use an approach for no other reason than it was used before in an unrelated situation. In addition, the Lawrence Livermore National Laboratory decontamination experts told us that decontamination costs can increase dramatically depending on the selection of an initial approach and the length of time before remediation actions are taken. For example, they said that the conventional use of high pressure water hosing to decontaminate a building is effective under normal conditions but could be the wrong clean-up approach for an RDD using cesium-137 because the force of the water would actually cause this radioactive isotope to penetrate even further into porous surfaces. A senior EPA official with the Office of Radiation and Indoor Air told us that studies are currently underway to determine the efficacy of pressure-washing for removing contamination from porous urban surfaces.

In addition to the lack of knowledge about the application of clean-up methods and technologies for wide-area urban contamination from an RDD or IND incident, there are also limitations in Federal capabilities to handle in a timely manner the magnitude of tasks and challenges that would be associated with these incidents. For example, we found that limitations in Federal capabilities to complete some analysis and clean-up activities might slow the recovery from an RDD or IND incident, including: (1) Characterizing the full extent of areas contaminated with radioactive materials; (2) completing laboratory validation of contaminated areas and levels of clean-up after applying decontamination approaches; and (3) removing and disposing of radioactive debris and waste. Respondents representing most of the cities (9 of 13) and States (7 of 10), and respondents from most FEMA regional offices (6 of 9) and almost all EPA regional offices (9 of 10) expressed concerns about the capabilities of Federal agencies to provide the assistance needed to complete the necessary analysis and clean-up activities in the event of an RDD or IND incident.

CITY, STATE, AND FEDERAL EMERGENCY MANAGEMENT OFFICIALS HAVE SEVERAL SUGGESTIONS TO IMPROVE FEDERAL RECOVERY PREPAREDNESS FOR RDD AND IND INCIDENTS

Respondents from nearly all the cities and States we surveyed expressed the need for a National disaster recovery strategy to address gaps and overlaps in current Federal guidance. According to one city official, "recovery is what it is all about." In developing such a recovery strategy, respondents from the cities, like those from their States, want the Federal Government to consult with them in the initial formulation of a recovery strategy through working and focus groups, perhaps organized on a regional basis. Respondents representing most cities (10 of 13) and States (7 of 10) also provided specifics on the type of planning guidance necessary, including integration and clarification of responsibilities among Federal, State, and local governments. For example, respondents from some of the cities sought better guidance on monitoring radioactivity levels, acceptable clean-up standards, and management of radioactive waste. Most respondents from cities expressed the need for greater planning interactions with the Federal Government and more exercises to test recovery plans. One city respondent cited the need for recovery exercises on a regional basis so the cities within the region might better exchange lessons learned. Respondents from most cities (11 of 13) and their States (7 of 10) said that they planned to conduct RDD and IND recovery exercises in the future. Finally, emergency management officials representing almost all cities and States in our survey offered some opinions on the need for intelligence information on RDD and IND threats. They said that sharing information with law enforcement agencies is necessary for appropriate planning for an RDD or IND incident—which they generally consider as low-level threats—but only half of the respondents indicated that they were getting sufficient intelligence information. Emergency management officials from FEMA and EPA regional offices generally concurred with these observations and suggestions of the city and State respondents.

THE UNITED KINGDOM'S HANDLING OF THE 2006 POLONIUM INCIDENT AND SUBSEQUENT ACTIONS TO BETTER PREPARE FOR AN RDD OR IND INCIDENT

While it was more limited in scope than what is usually envisioned as an RDD incident, the aftermath of the 2006 polonium poisoning incident in London had many of the characteristics of an RDD including testing hundreds of people who may have been exposed to radiation and a clean-up of numerous radiation-contaminated areas. All this activity resulted from an amount of radioactive material the size of a grain of salt—many times smaller than the amount of radioactive material found in certain common medical devices that could be used in an RDD. Because of its experience in dealing with the clean-up from the 2006 polonium incident and other actions the United Kingdom has taken to prepare for an RDD or IND attack, we visited that country to examine its recovery preparedness programs. United Kingdom officials told us that the attention to recovery in their country is rooted in decades of experience with the conflict in Northern Ireland, dealing with widespread contamination from the Chernobyl nuclear power plant accident, and a national history of resilience—that is, the ability to manage and recover from hardship. We found that actions the United Kingdom reported taking to prepare for recovery from RDD and IND incidents are similar to many of the suggestions for improvement in Federal preparedness that we obtained through our survey of city, State, and Federal regional office emergency management officials in the United States. For example, we found that the United Kingdom reported taking the following actions:

- Enacted civil protection legislation in 2004, with subsequent non-statutory emergency response and recovery guidance to complement this emergency preparedness legislation. The emergency response and recovery guidance describes the generic framework for multi-agency response and recovery for all levels of government. The guidance emphasizes that response and recovery are not discrete activities and do not occur sequentially, rather recovery should be an integral part of response from the very beginning, as actions taken at all times can influence longer-term outcomes of the communities.
- Developed on-line, updatable national recovery guidance in 2007. This guidance reinforces and updates the early emergency response and recovery guidance by establishing, among other things, a recovery planning process during the response phase so that the potential impacts of early advice and actions are explored and understood for the future recovery of the affected areas.
- Issued a national handbook for radiation incidents in 2008. This handbook provides scientific information, including checklists for planning in advance of an

incident, fact sheets on decontamination approaches, and advice on how to select and combine management of these approaches.

- Conducted a full-scale RDD recovery exercise in 2008. This exercise, involving several hundred participants, provided a unique opportunity to examine and test the recovery planning process within the urgency of a compressed time frame. The lessons learned from this exercise were incorporated into the United Kingdom's recovery strategy.
- Issued updated nuclear recovery plan guidance in 2009. This guidance provides direction on recovery from events involving a radiological release from a civil or defense nuclear reactor, as well as the malicious use of radiological or nuclear materials. Among other things, it requires that all high-risk cities in the United Kingdom prepare recovery plans for such incidents.

In addition to these initiatives, in 2005, the United Kingdom established a special Government Decontamination Service. This organization was created out of recognition that it would not be cost-effective for each entity—national, regional, and local government—to maintain the level of expertise needed for cleaning up chemical, biological, radiological, and nuclear materials, given that such events are rare.[19]

Finally, according to United Kingdom officials, the 2006 polonium incident in London showed the value of recovery planning. In particular, through this incident United Kingdom officials gained an appreciation for the need to have an established clean-up plan, including a process for determining clean-up levels, sufficient laboratory capacity to analyze a large quantity of samples for radiation, and procedures for handling the radioactive waste. Furthermore, they found that implementing clean-up plans in the polonium poisoning incident and testing plans in the November 2008 recovery exercise have helped the United Kingdom to better prepare for a larger RDD or IND incident.

Madame Chairwoman, this completes my prepared statement. I would be happy to respond to any questions that you or other Members of the subcommittee may have at this time. For further information about this testimony, please contact me.

Ms. CLARKE. Thank you very much, Mr. Aloise.

We are going to break with the protocol. One of my colleagues has to leave a bit earlier. I would like to then recognize for 5 minutes the gentlewoman from California, Ms. Laura Richardson, for her questions at this time.

Ms. RICHARDSON. Thank you, Madam Chairwoman and also Ranking Member Lungren, for allowing me to kick off first. I have a 1 o'clock flight, and I have to get to the airport, so I appreciate it. Thank you.

You know, I am a relatively new Member on the Homeland Security Committee, even though my district is very rich in targets. When I first heard the initial testimony of Mr. Conklin, when you said we need a coordinated Nation-wide program, I was somewhat surprised, given, you know, how many years now we have been working in this effort.

Would you like to expand further on what you would more like to see? I thought Mr. Aloise's comments were excellent.

Mr. CONKLIN. Well, the program that I am talking about is a program that was established by HSPD–7 for addressing the security of the Nation's critical infrastructure and key resources. That program was kicked off about 5 years ago in formality with the HSPD–7, but it started well before that.

In the nuclear section, in particular, we have established a partnership framework that involves what we call a Government Coordinating Council of the Federal departments and agencies, as well as State representation. We work with a private-sector coordinating council, which has representatives from the power plants, manufacturers of portable sources, the representatives from the re-

[19] The Government Decontamination Service is similar in size and responsibilities to EPA's National Decontamination Team, which became fully operational in August 2007.

search and test reactors, from the universities and things like that. So that is the framework that I am talking about.

Now, if you are talking about a bigger framework, the Federal Government has been involved in radiation protection issues, emergency response issues for years. Following TMI, for example, FEMA was assigned responsibilities to establish a Federal Radiological Preparedness Coordinating Committee. Their initial focus was the commercial power plants, but over the years they have expanded that focus into foreign accidents involving radioactive material, lost or orphan sources of radioactive material.

So there has been a fair amount of effort going on to address these issues. Now, are we there yet? Do we have a system in place that we can point to that says we can answer all the questions and do everything that is going to be needed? I would have to agree with the gentleman at the other end of the table that that is not the case.

There are still significant areas that need improvement with regard to risk communication, the ability to detect the material once it has been used, and then the follow-on and clean-up. It is going to be a massive effort to do that clean-up and recovery; there is no question that.

Ms. RICHARDSON. Okay. Thank you.

Mr. Sheely, as I was listening to your testimony and also reading the GTRI remote monitoring system, and when I looked under the initiatives it said that, "Upon request, perform security assessments and upgrades." This is all to be done by 2016, which I thought was a little odd that it would be upon request.

Then it had here that you estimate that 2,200 buildings in the United States house Category 1 or 2 levels of materials. We have only done 37 buildings so far.

Do you think we can really meet this goal by 2016? It is almost like fixing infrastructure to me. By the time you get there, it would seem like you would have to do it all over again. So is this realistic, the way that we are doing it?

Mr. SHEELY. Well, no, that is a very good question. As you said, it is a very complex issue. But we feel pretty confident. We have been doing security best practices overseas for many years, as far as the GTRI program. It was actually a fairly recent GAO study done by Mr. Aloise's group saying, who was offering those same kinds of best practices to source holders here in the United States? That just recently, within the last year or so, that we have really been partnering with NRC and DHS to offer such activities. Right now, we actually have more volunteers than resources available to address those volunteers.

Ms. RICHARDSON. I am sorry. Here in Congress, we run pretty tight on time frames. Mr. Conklin took a while. I have 1 minute.

My question is, right now you say we have 2,200 buildings that need to be evaluated and only 37 have been done. Do you think it is possible that we are going to achieve that?

I am sorry; I just want to respect my colleagues.

Mr. SHEELY. Okay. I think it is possible to achieve it because we have just begun the program, and it is expanding quickly.

Ms. RICHARDSON. Okay. Will it have to be done again after 2016? Is it something that is done repeatedly?

Mr. SHEELY. It should not have to be redone again, no.

Ms. RICHARDSON. Okay. Then, how many cities do we know have participated in the Securing the Cities Initiative? Does anyone know that?

Mr. RIGGIO. There are 150, approximately, maybe 154 law enforcement agencies across those three States. It encompasses approximately 60 counties. Because there is cross-jurisdiction with sheriffs' offices and small townships, I couldn't give you an exact number of cities.

Ms. RICHARDSON. But that is just within the three cities that you are working with. That is not all the cities in general.

Mr. RIGGIO. No, the three States. New York——

Ms. RICHARDSON. Three States, okay.

Mr. RIGGIO. Yes. Picture Manhattan as the focal point, and expand in a radius, a circular radius, outside. You pick up Long Island, Connecticut, upstate New York, and New Jersey all around.

Ms. RICHARDSON. But are other cities across the country doing the same thing?

Mr. RIGGIO. To my knowledge, the New York-area Securing the Cities Initiative is the first, and it has not been expanded at this point.

Ms. RICHARDSON. Okay.

Thank you very much, Madame Chairwoman.

Ms. CLARKE. Thank you, Ms. Richardson.

I want to once again just thank our witnesses for their testimony.

I remind each Member that he or she will have 5 minutes to question the panel. I will now recognize myself for questions.

My first question is to Mr. Conklin. One issue we on the committee struggle with is in protecting our infrastructure and providing for security of privately held assets.

Were our voluntary efforts effective, or where do we need to regulate? In the case of source security, have voluntary efforts really been enough, or have you benefited from the fact that the NRC is there to provide regulation when needed?

Mr. Levis, would you care to comment on that?

Mr. LEWIS. Well, thank you for the question.

I think that these two programs do complement each other. The NRC's increased controls set a baseline of safety. The security assistance and the hardening that are done are voluntary measures that go beyond the minimum requirements for security that apply to everybody. Those requirements reflect best practices for a particular type of licensee, geographical issues such as what is specific to New York, and other factors. I do think they complement.

We are undergoing a regulation change. In the spring of next year, we expect to issue new regulations on materials security. One of the things we will be seeking in the proposed regulation is feedback on how the voluntary measures and the increased controls, which are required measures, complement each other or not and can be used to the same goal.

The voluntary measures have the advantage of being able to be done more expeditiously than if NRC were to require them. We would have to do a regulatory change, and then there is no longer a central place dealing with the vendors to enact the changes. It

would be decentralized, where all the licensees would do it themselves.

Ms. CLARKE. Mr. Conklin, do you have anything to add?

Mr. CONKLIN. I would definitely say that the voluntary program has benefited from those regulations. Having a baseline of activity that has preceded our coming into the program, if you will, for years really helped identify where we stand and established a good starting point from which to then elevate the level of protection that we wanted for these sources.

Ms. CLARKE. Very well.

Captain Riggio, in August, an iridium source was reported missing here in New York. The source was recovered within 2 days.

Can you please tell us about the incident and please indicate whether any of the enhanced security measures, including updated tracking procedures, helped in recovering the source, or did you have significant Federal and State cooperation?

Mr. RIGGIO. Madame Chairwoman, with respect to that incident, essentially what happened, on the morning of the incident, the office manager came into the facility, did the morning routine, the facility inspection, and noticed a piece of equipment missing.

Nine-one-one was immediately called. Routine patrol officers responded to the scene. When we realized what, in fact, we were dealing with, obviously more enhanced and specialized units were called: The counterterrorism division, the joint terrorism task force.

To get to your question, some of the measures that were put in absolutely helped in recovering it, because, without getting into too much for operational security, certain codes had to be put in to get into the facility. There were some cameras that were working, and so we were able to figure out maybe which individuals had come in in recent hours and get some sort of picture from a videocamera afterwards.

So, yes, certain things did help in the recovery, yes, and the quick identification of where it might be and leading us to persons who may be of interest using other computer systems that we have, where, in fact, they may be located and where to put our resources to try to find them.

Ms. CLARKE. Thank you.

Mr. Sheely, we have been pleased to see the progress made in getting the engineering upgrades placed on over 20 blood irradiator machines. It is my impression that the fact that DOE is providing these free of charge has been a big key to your success.

Do you feel that providing these for free is essential, even though the upgrades range from $5,000 to $20,000 a piece, which seems like a very small investment for a major hospital?

Mr. SHEELY. Yes, we do feel that, again, offering these free of charge, as Mr. Lewis mentioned, is really accelerating the ability to secure these cesium irradiators much more quickly.

As I am sure other colleagues would atone, many of these hospitals, especially the large hospitals, have on the order of six or seven or even eight of these large irradiators. The costs do add up when you have that many. It is always a trade-off, whether it is a university setting, a hospital setting, or in the case of the facility where we are now is both, there is always a trade-off between patient care and security upgrades.

So we do feel that this is a very valuable service which will ultimately result in the quickest security upgrades.

Ms. CLARKE. Thank you.

I now recognize the Ranking Member of the subcommittee, the gentleman from California, Mr. Lungren, for his questions at this time.

Mr. LUNGREN. Thank you very much, Madame Chairwoman.

I want to thank all of you for your testimony. I had an enjoyable ride on the train up here and got to read it all, and it was very, very helpful, and I appreciate it.

Mr. Conklin, Mr. Sheely, Mr. Lewis, how much, if at all, is the problem that you have articulated exacerbated by nuclear radiological waste at hospitals and other institutions?

Mr. CONKLIN. Well, I will kick it off.

I think the biggest concern we have is a small percentage of the radiological waste, and that deals with the actually sealed sources themselves that either through the use of their lifetime they lose their strength and therefore they are not suitable for doing the job they are doing.

The ability to dispose of those, the cost has gone up, the options have gone down. So there is a tendency, or there could be a tendency, to accumulate this waste and store it on-site versus pay the cost for getting rid of it.

Mr. LUNGREN. You say there could be a tendency. Is there a tendency?

Mr. CONKLIN. I believe there is, yes.

Mr. LUNGREN. Mr. Sheely.

Mr. SHEELY. Well, as Craig was mentioning, I think the main issue is that approximately less than 1 percent of the overall medical waste is useful in an RDD-type dispersion. So, in that sense, from a security standpoint, the risk is manageable, and the key is to separate those sources which are Category 1, 2 sources, which could be used in an RDD, from just other medical radioactive waste.

Mr. LEWIS. There is a lack of disposal access for these sources. They are low-level waste. They are not nuclear waste or high-level waste. But they are greater than Class C low-level waste, which means they are not suitable for near-surface disposal, and there is no facility that can take those at this time.

Mr. LUNGREN. So where do they go? What do they do?

Mr. LEWIS. They are stored or returned to vendors. Fortunately, they are small in number and volume, so storage is an option.

Mr. LUNGREN. Dr. Arquilla, what do we need to do to bring our country up to the level that you would like to see, with respect to preparation of our hospitals for responding to an event if it should happen, No. 1; and, No. 2, doing a better job of informing people of exactly what a dirty bomb is and what it is not?

As you say, 65 percent, I believe it was, of the people would self-evacuate, which sounds good. But it is also bad because, when they evacuate, they are going to go to the hospital. As I understand your testimony, most would probably need not go to the hospital, at least not go to the hospital immediately.

Dr. ARQUILLA. Probably the most important, best thing is to start with educating the population in general about, you know, what ra-

diation is. We have 70 years of "You are all going to get radiated and turned into a carrot." So I think that that would be one step.

I mean, if you look at curriculums within nursing schools, medical schools, there is very little in this kind of education. Unless you going into radiation oncology, you really don't know anything about it. So, to me, it would be to go from both directions, it would need to be that.

I think that kind of risk communication is not that difficult, but it is not happening. It is more hysteria education than it is—you know, most physicists aren't worried at all about this. They think we are kind of crazy to be so upset, you know, if you actually sit down and speak with them.

Getting that across is a generational thing, but I think that that would be the most important thing. We have nonfunded mandates to do this education. We can't do it like that.

Mr. LUNGREN. Captain Riggio, your testimony is impressive with respect to what the NYPD can do. It has often been observed that you have many more officers per population than just about any community in the United States. I reflect when I used to represent the southern California area and when I was attorney general, I remember the comparisons of LAPD versus NYPD.

The reason why I bring that up is, you folks have done a great job of coordinating and having your own special units and so forth. Is that actually replicable in other parts of the country? Are there lessons that can be learned from your experience even though very few departments, if any, can replicate your organization and the detail of your units and subunits?

Mr. RIGGIO. I believe it can. I mean, obviously, having personnel above and beyond what everyone else has is a great advantage. But that being said, you know, we live in a time where we can't use personnel resources as an excuse. So there are absolutely lessons that—and that is kind of what the Securing the Cities program has done.

Many of the departments that we work with are smaller in size than us, but we pass along the lessons that we have learned, whether it be source security, interdiction methods, setting up chokepoints, how we run everything, all of our terrorism, not just radiological, CBRNE, different trainings and practice.

So it can be replicated, to answer your question. It is difficult. I know, I am sure, that in this time, if you ask many of these agencies, they will talk about fiscal responsibility and fiscal crisis that we are in now and that they would need help to do these things. But I do believe it is absolutely replicable.

I mean, that is something that we like and we wish. Because we see it as, yes, while New York City is the target, what happens in Pennsylvania and Ohio affects us, because something can happen there and they come over and bring it over to us.

So I hope I answered your question, sir.

Ms. CLARKE. I now recognize the gentlelady from California, Ms. Sanchez, for 5 minutes.

Ms. SANCHEZ. Thank you, Madame Chairwoman.

Again, once again, thank you all. You seem to have a great array of people here in New York, in the New York area, with respect to this issue. I applaud both you, Ms. Clarke, for holding this hear-

ing, for having these types of experts here. It has been very enlightening this morning.

I also want to thank, of course, our Federal people who were here, who I know are on the front line every single day, trying to figure out how we make all of this happen correctly.

I represent Orange County, California. That could be Disneyland, Anaheim Stadium, the largest convention center west of the Mississippi, the third venue in the Nation for concerts being our Honda Center, Knotts Berry Farm. I am about 20 minutes away from the Long Beach and Los Angeles ports, which Ms. Richardson has in her backyard, and aside some beautiful beaches.

So you can imagine the type of concentration of people in my area every single day of the year that don't necessarily live there but who come in for the day or come in for the week—much in the same way as we might see New York City, with its influx of visitors. So we are very, very concerned about so many of these issues.

In identifying—I have been in the Congress 13 years, when this committee was set up. I am the vice chair of the Homeland Security Committee. We identified our main venues. For example, I will start with Disneyland, where they said if something goes off in the park, maybe it affects 10,000 people in the vicinity of the park, but 60,000 people who live within a mile of Disneyland will be rushing to my emergency room at my hospital, which of course might have two beds open, as we speak right now, because there is such a crunch. So we started working with UC-Irvine, in particular, which is my hospital there in trauma and hospital of the vicinity, to work on these issues.

Doctor, you mentioned that you didn't think there was anybody who had a decontamination, sort of, 24-hour process going on. I might urge you to talk to them, because we just built the new hospital. They don't have 24-hour, on-the-line team, but they do have probably the best thing in the Nation that one could have for that. So I would—I don't know if you are talking to them.

Dr. ARQUILLA. I am talking about personnel, not about toys.

Ms. SANCHEZ. We are talking about personnel also. They have——

Dr. ARQUILLA. I graduated from Irvine. I know it very well.

Ms. SANCHEZ. They have done a pretty good job over there, so I just wanted to mention that.

But my big issue is this issue about, how do we talk to our people? I mean, how do I tell my people who are living within a mile of Disneyland—and I do—that if they hear something on the radio happening at Disneyland, that they don't rush down to the hospital? What do you think is the most effective way?

I also want to hear from Captain Riggio, because local law enforcement are the ones who have to handle this herd mentality of, "Oh, my God, the world is ending. Let's get to the place."

How do you suggest we do that? Have you seen resources? How are you dividing your resources and trying to communicate or getting this information out to the general public?

Dr. ARQUILLA. One way that I see to do it is, prior to an event, we really need to start look at the emergency care as not an excuse for a clinic. That would be one thing on a regular basis across the

board for all CBRNEs. Remember "B" is "biologic," and we are looking at a big flu season this year.

So, to educate people as to what hospitals can and can't do, prior to the event. I think that, within New York City public schools, they are actually trying to pilot some ideas on that, you know, when to go to the hospital, when not, for the parents and those issues.

I don't think—I mean, it may be a health care issue, but I can only say that, unless we create liaisons with other organizations, be it news, first responder, which was fire, police, whatever, to let them know about risk management and really what the risks are, because they are very different risks than what we think, then I don't have a perfect excuse.

But I do think education of our risks and understanding our risks in this kind of a committee, where we are really evaluating risk, I think is key.

Ms. SANCHEZ. Captain.

Mr. RIGGIO. To answer your question, our primary goal, our mission, is to prevent, obviously, something from happening. In the event that something would happen, then our goal becomes to mitigate and save as many lives as possible on the scene.

As far as the question that I think you are asking——

Ms. SANCHEZ. How is your salary paid, for example? Is it coming in from Federal grants? Is it coming in from a State grant? Is it a body at the police station now that has to be put over to this?

Mr. RIGGIO. No, I am—you know, we have a budget, the city has a budget, that accounts for the personnel within the New York City Police Department, and I am just one of them.

Ms. SANCHEZ. So every time that we pull you away from crime-fighting because we need to do this, we need to ensure that is moneys that you all are spending out of your own pocket, that, you know, we expect you to be doing all this but there is no real money in it?

Mr. RIGGIO. You know, Federal funding is an issue that comes up. My duties are 100 percent solely to counterterrorism, and so that is my function. Twice a month, I do go back to patrol. But, essentially, my duties are strictly for counterterrorism.

I apologize, I am not sure which question I am trying to answer here.

Ms. SANCHEZ. I am trying to figure out, in a time of a lack of resources, at a time when we don't have as many people as we want on the beat, if you will, how we are going to fund pulling people away from their basic mission, which is stop the bad guys, to education, synergy, having plans in place and action also. I am trying to figure out where you are getting the money to do this.

Mr. RIGGIO. Well, like I said, we budget it through two channels: Through the city's budget, which comes from taxes right here within the city tax base, and, you know, fortunately, we look to get a lot of Federal funding, as well. I mean, we apply for grants just like everybody else, and we push and we push and we push, because we know that it takes two parts, it takes multi-jurisdictions to get this done.

We couldn't do it on our own. That is certainly for sure. In this day and age, we can't. We know what the environment is going to

look like ever since September 11. Nothing is going to change. The mentality that we have, as far as, "work, work, work, don't stop, you have to keep being on top of this," it is not going to change. It is not going to change, as long as I am going. So there needs to be a combination of city resources and Federal resources, as well.

Ms. SANCHEZ. Thank you, Madame Chairwoman.

I actually have one more question. May I ask it at this point?

This has to do with—and I guess I would like to bring our GAO specialist here. We just had a study done at the State level in California with respect to where the homeland security moneys are from the State. You know, pretty much, we send a lot of the Federal moneys to the State, and the State gets it down, supposedly, to the local levels. It was a pretty scathing report about how jurisdictions are spending the money that is given to them.

In particular, some say, well, you know, I mean, if you are going to give me $90 because it is on a population-based formula or something and so I am a little city, I am going to get something, yes, I am going to buy, you know, ventilation something or another that costs $89. I mean, it is not really significant towards what we are really trying to do, in some ways. This study basically said people are just spending money because it is there, and they are spending it and they are not really that strategic.

I am not saying all of them. I think I have, you know, Mutual Aid and Sheriff Baca out there and everything that we have going. But would it be more effective—I would like to ask to our GAO specialist—have we seen this at Federal level? Have we done a type of study recently that speaks to where the moneys from the homeland security grants and things are going to and how effective they have been?

One of the reasons that I hear from local agencies as to why they are buying things is because, to a large extent, they are not allowed to spend it on people, on personnel.

Can you talk a little to that? I don't know if it is your area of expertise, if there is a study, if I just haven't seen it or I have forgotten that I read it. Have we done it recently? Do you have any comment with respect to this buying things versus maybe putting the money more towards personnel?

Mr. ALOISE. Let me try to answer that based on the work that we have done in this area. There probably is a study; I will check and get back to you if I find one.

What we found, talking to people at the Federal, State, and local level, is that the State and local folks, when they get this money, what they need is some guidance on what to buy, what makes sense, and they are not getting that from the Federal level. They need more help in terms of, what are we supposed to defend against and what is the best equipment to buy? Sometimes they just end up buying stuff because they don't know what the right thing is to buy.

We have talked about this a lot in reports, that they need more Federal guidance on what are the best ways, most efficient ways to spend money, on what equipment. So there is a need to get help to these people in terms of guidance at the State and local levels.

Ms. SANCHEZ. Great. Thank you.

Thank you for your indulgence, Madame Chairwoman.

Ms. CLARKE. We are going to do another round of questioning. I hope that our witnesses will be able to just hang in there with us. This is very intriguing, very important information that this subcommittee needs.

I want to go to Mr. Miskin and ask for—can you give us an update as to the installation of engineering upgrades in New York City hospitals? Is New York complete as far as these upgrades are concerned? If not, when you do anticipate that all of the irradiators in the city will have these security upgrades? Do you feel that Federal agencies have been effective in working with you to achieve this goal?

Mr. MISKIN. Madame Chairwoman, we have had three facilities that were part of a pilot project in 2008 to have their cesium chloride blood irradiators hardened. I understand that we will be visited soon by NNSA to see if other facilities in the city need to be upgraded and hardened, and we will be working with them.

Ms. CLARKE. So it is not quite complete as of yet?

Mr. MISKIN. It is not.

Ms. CLARKE. Okay. Okay.

Let me then turn to Mr. Aloise. I will ask you a question about the challenges that cities would face with an RDD attack using cesium chloride as a source and the medical response. I think it is important for us to understand what we will be dealing with should one of these sources be stolen and used as a dirty bomb.

What are the critical challenges and difficulties in recovering from an RDD attack, specifically using cesium chloride as a source?

Mr. ALOISE. Well, one of the problems with cesium—and this is why recovery planning is so important, because recovery planning starts in the response. We need to know how to clean up some of these areas. Cesium, in particular, if you do it the wrong way, it is going to end up costing you more money, and you may have to demolish a building rather than just clean it up. If you use a high-pressure hose on cesium, it actually pushes it further into the building and makes the condition worse.

So there has to be—in the response phase, there has to be that recovery planning. After we have characterized what the material is, determine the best way to clean it up, and let the first responders know, "On this particular building, you are not supposed to use a high-pressure hose because that makes things worse."

Ms. CLARKE. Very well. I think, you know, that, in combination with the concern that Ms. Sanchez has about what we are purchasing, what we are actually teaching or giving guidance to with regard to jurisdictions around this Nation, it compounds the problem.

Without the proper training and education and the purchasing of just, you know, equipment for equipment's sake, we are really building up a false sense of security in certain jurisdictions around this Nation. I think it is really important that DHS, sort of, gets on top of this.

Let me just ask that similar question. I see you are back, Dr. Arquilla. What would you say are the most significant challenges that the city would face if there were an RDD attack using cesium chloride as a source, as far as the medical response?

Dr. ARQUILLA. I mean, it is a really nasty radiation, so there will be sick people. I think that is the No. 1 thing. If I were to really boil it down, the greatest challenge is who is sick and who is not and being able to tell. Also, looking at, you know, who needs to be watched. If we were to, you know, use something like a blood test, then that means we are testing thousands and thousands of people and also waiting for the results to get back.

So I think probably, from a medical point of view, the big challenge is who is sick, who is not sick, who needs to be watched and for how long. Some studies say you need to watch people for 25 years. You know, that is a huge, a huge question that you have to look at.

Just one other thing, too, is, if you were to, like, say, "Okay, I don't know anything this, let me go to the CDC website and look it up," there are probably, oh, hundreds of documents on it. There is no easy, like, let me find it, this is yes, this is no. I think that that—you know, it is like too much knowledge is almost another part of what is going on.

Thank you.

Ms. CLARKE. Thank you.

I now recognize our Ranking Member, Mr. Lungren from California, for his questions at this time.

Mr. LUNGREN. Thank you, Madame Chairwoman.

In terms of replicating things, you ought to contact the people who manufacture your hand dryers in there. I went to the restroom, and I thought that there was a high-pressure hose in there. Either that or a jet engine. I have never heard so much noise. It dried my hands completely. So talk to those folks.

Captain, when you talk about way of paying for these things, I looked at my bill from the hotel, and we are doing our part. We are paying the State $32, we are paying the city $21, and then you have an occupancy tax of $3.50.

Mr. RIGGIO. We thank you for that.

Mr. LUNGREN. It may be helping your salary.

I think some people don't appreciate the Securing the Cities program. That is a program that is specifically for this three-State region. It is something that was supposed to be a seed money program. It has discontinued, although I know a number of people in the New York delegation are working hard for it. Peter King and I have spoken out for it, because I do think what you are doing here is important. But more than that, I think it does give us some examples of what we must and can do around the country.

Ms. CLARKE. Will the gentleman yield just a minute?

Mr. LUNGREN. Yes, I would be happy to.

Ms. CLARKE. Yes, we were successful in getting the funding put into the appropriations bill. Hopefully it will remain through the Senate reconciliation.

Mr. LUNGREN. So, I mean, it is important for us to understand what you are doing with these funds and how it is working in an effective way.

One of the things I noted in your testimony, you talked about surveys and security recommendations, almost 100 facilities within the city of New York. Are those only medical facilities, or are they industrial facilities?

If they are industrial facilities, was the industrial facility in which you discovered that industrial radiograph missing one of those that you have given special attention to?

Mr. RIGGIO. It was. The locations that I spoke about were combined; it was medical and industrial facilities. That was a facility that we had visited in the past. So we——

Mr. LUNGREN. Is it a concern of yours that it is one of those that you visited in the past that had the understanding that they should report something like this to you right away? Or do you feel that that would be reported to your folks as a theft or missing inventory with the dispatch that this was reported to you?

Mr. RIGGIO. We were happy with the reporting here, that it happened so quickly. Obviously, what we found out after the investigation we were not happy with. This practice that we are trying to uncover as to, is there more that happens with these employees once they get off?

But as far as the reporting, I mean, they did exactly what they should. They came in; they noticed this right away. They called 9–1–1.

We handled it on two fronts: We handled internally within our city and what we needed to do to try to locate is this. But, also, the reason the Securing the Cities program exists is for situations just like this. So we actually initiated a Securing the Cities conference call and brought all our partners into what was happening and had them stand up to a certain level, as well.

Mr. LUNGREN. One of the reasons why it is important to have this testimony from this panel is that, in the Congress, we have done something over the last number of years since 9/11 which is a little different. We have tried to use homeland security funds, programs, on a bipartisan basis that are risk-based as opposed to strict population formula-based. That debate continues to rage, and it is raised every single year.

Because you have to understand, oftentimes there is a notion that funding ought to go fairly to everybody, no matter what the risk is. It is important for us to remind ourselves that risk-based funding is not only important from the standpoint of those of us in Congress, but also the Executive branch carrying that out, and then at the local and regional levels, that they understand that is what the focus of these programs are.

So, Mr. Aloise, you indicated in your testimony that the GAO survey of agencies from these exercises that have occurred on the State and municipal level has revealed, I believe your language is, "an overreliance on Federal help and the lack of Federal planning in the event of an attack."

Can you talk about that a little bit more?

Mr. ALOISE. Yes, I am talking about recovery planning. There has been lots of attention placed on response, not enough on recovery yet. I think our first exercise won't be until 2010 on recovery. Most of the State and local people we surveyed see the need for that, want the involvement of Federal Government, want more interaction, including New York State, with the Federal Government on planning.

As I mentioned earlier, part of a successful response is to have your recovery planning into that, so you are not doing things that are going to cause you problems in the long term.

Mr. LUNGREN. Here we are in New York. You were ground zero, this city. We have just gone through the anniversary of 9/11. One of the concerns that I have had and continue to have is the lack of urgency we have, both on the Federal level and in local levels. We haven't had an attack since 9/11 so we have let our guard down. That would be the wrong message.

I hope what we are talking about here with this specific problem is that we have to maintain or re-establish that urgency, but do it in an intelligent way, as Dr. Arquilla says. Let's understand what the threat is, not overhype it, not underestimate it, but know what the facts are and then deal with those facts.

So I thank you for your testimony. It has helped us very, very much.

Thank you, Madame Chairwoman.

Ms. SANCHEZ. Madame Chairwoman.

Ms. CLARKE. Yes, Ms. Sanchez.

Ms. SANCHEZ. Madame Chairwoman, because of the time constraints, I will be submitting some questions for the record for the witnesses to answer, if that is okay with you.

Ms. CLARKE. Before we conclude, I would just also like to ask unanimous consent to submit a statement by the IP Radiation Associates to the record.

Hearing no objection, so ordered.

[The information follows:]

STATEMENT OF IP RADIATION SECURITY ASSOCIATES

Dear Chairwoman Clarke and Members of the subcommittee: My name is Keith Reynolds and I am the founder and principal of IP Radiation Security Associates. I am also a co-founder of a company that develops software to improve response procedures in the case of a radiological event. I continue to work with Internet Protocol-based security and radiation instrumentation companies to make our world safer from criminal use of radiological materials. We are employing Internet Protocol (IP) technologies to tie commercial, off-the-shelf (COTS) security systems together with a variety of radiation detectors.

By networking radiation and various other COTS security systems we can enhance the security of radiological sources, improve first responder's ability to react to a radiological event and reduce costs compared to proprietary detection systems. The implementation of IP Radiation Security (IPRS) systems is especially important to the programs like the Global Threat Reduction Initiative (GTRI) and those considered under House Bill HR 2070, the Radiological Materials Security Act introduced by Chairwoman Clarke. As taxpayers we will be afforded greater protection for the money spent in this critical area.

The threat of terrorists abusing radioactive materials is grave. The sheer availability of sources in facilities employing less than optimal security programs creates a need for more public and private investment in new security systems. We must also rethink how security is implemented based on the improvements new technologies enable. Such changes necessitate new knowledge and training to be sure. However, the risk posed by the status quo is high. In my own work over the last several years I have been in situations where I have had access to significant amounts of radiological materials in facilities I would consider less than secure.

I submit this statement for the record to highlight the threats posed by radiological sources and offer a cost-effective solution for Government and private efforts to secure them.

THE THREAT POSED BY LEGITIMATE RADIOLOGICAL MATERIALS

In the United States of America alone, there are nearly 23,000 licensees using radiological materials. These users are charged with the security of roughly 2 million sources. There are some 10 million sources worldwide.

Radiological materials can uniquely help solve the world's food, energy, environmental, and cancer problems. However, growing use of radiological material in these sectors, combined with the global threat of terrorism, has increased the risk of unwanted radiation exposure. Accordingly, radiation security has become as important, if not more important, than the traditional Radiation Safety model, which has existed for over 50 years.

A small amount of conventional explosives combined with stolen radiological material is enough to create a "dirty bomb" (or RDD, short for Radiological Dispersion Device). One thousand curies of Cesium-137 (Cs-137) could fit in a soda can. Between 50 and 100 curies of Cs-137 is enough to make a RDD that could shut a Grand Central Station-sized building for a year or more as crews clean up the facility to achieve Federally mandated background radiation levels.

A dirty bomb would not likely kill large numbers of people from radiation poisoning. Such a device would certainly cause massive economic disruption. Estimates are for up to $100 billion to clean up dispersed material [1] and as high as trillions in economic losses.[2] A "Radiological Emissions Device," where a relatively small amount of radiological material is left in a public facility, presents a scenario that could potentially injure or kill hundreds of people. Widespread societal panic will surely ensue in both cases.

THE PROBLEM OF LOST OR STOLEN SOURCES AND ILLICIT TRAFFICKING

The International Atomic Energy Agency (IAEA) has recorded 1,562 nuclear trafficking incidents from 1993 through 2008. Worldwide, the number of reported cases of lost and stolen radiological materials has been increasing according to the IAEA. These incidents range from illegal efforts to dispose of radioactive materials, to discovery of "orphaned" nuclear material of unknown origin. In its 2008 annual report released in August of this year, the IAEA received reports of 15 cases of clandestine nuclear possession, or related incidents and 16 cases involving theft or loss of sensitive substances. According to the IAEA, these incidents are part of 119 events that were added to the IAEA's Illicit Trafficking Database in 2008, while this year to June, the agency has received reports of 215 incidents. That is up from 85, 2 years prior, though the IAEA does have participation by additional countries.

In an August 1, 2007 NY Times editorial entitled "Seize the Cesium" by PETER D. ZIMMERMAN, JAMES M. ACTON and M. BROOKE ROGERS: "In the United States, commercial users lose about one radioactive source a Day . . . through theft, accidents or poor paperwork. One of these is recovered perhaps every two days, either because the radioactive materials are voluntarily returned or because of good detective work."

I have been studying the daily incident report activity posted on the website of the Nuclear Regulatory Commission (NRC). Besides Cs-137, of greatest concern to me is the number of incidents involving significant amounts (30–100 Curies) of Iridium-192 (Ir-192) being deployed in the field of radiography for applications such as verifying pipeline welds. This survey of the NRC database of reported incidents over the last several months show just how prone to human error security is and highlights there is room for improvement. I submit for the record one of these incidents where an improved security system that integrates radiation detection, surveillance and communications could have helped. More are posted with comments on our website, *www.IPradiationsecurity.com* (with commentary) and at *www.nrc.gov*.

WEAPONS OF MASS DESTRUCTION

The Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism's Report to U.S. Congress submitted December 3, 2008, quoted Dr. Mohamed ElBaradei, Director General of the International Atomic Energy Agency (IAEA) speaking to the United Nations General Assembly on October 28, 2008: "The possibility of terrorists obtaining nuclear or other radioactive material remains a grave threat . . . It is more likely than not that a weapon of mass destruction will

[1] "Public Still in the Dark When it Comes to Dirty Bomb Threat", by Stew Magnuson June 2008.

[2] "Testimony of Dr. Henry Kelly, President Federation of American Scientists before the Senate Committee on Foreign Relations", March 6, 2002. On-line at: *http://www.fas.org/ssp/docs/kelly_testimony_030602.pdf*.

be used in a terrorist attack somewhere in the world by the end of 2013." In my own opinion, a RDD is probably the most likely weapon to be used.

Programs to mitigate "loose," or under-protected source materials are growing at home and abroad. In the United States of America, we have seen the NRC promulgate the Orders of Increased Control, GTRI has seen increased funding and the Radiological Materials Security Act has been introduced a second time. Abroad, radiological security has become a way for President Obama to engage the world from a foreign policy standpoint. Not only does the president advocate for the reduction of nuclear weapons through arms reduction agreements, but there is also a significant effort underway through these discussions to increase security of all other radiological material that are at risk.

Funding security enhancements and implementing networked radiation-monitoring systems that are interoperable with the security systems already in place are two large challenges that we face in addressing these security questions. Internet Protocol (IP)-based radiation detection systems can help make our Nation safer from radiological abuse by lowering costs and facilitating systems integration—just as the internet has revolutionized many aspects of our society, we can apply these technologies to do a better, faster, and more cost-effective job protecting ourselves from the threats of radiological terrorism.

WHAT IS IP RADIATION SECURITY?

A fully integrated enterprise security system provides near real-time monitoring of persons who enter facilities that house radiological materials and enhances control and reporting capabilities. Such systems integrate and utilize information from many discreet security systems.

IPRS combines digital, or "IP-enabled" radiation monitoring systems with other IP security tools, such as video surveillance, access control, motion detection, and the enterprise security management software in an integrated solution, or "systems of systems" approach. By combining specialized tools it is possible to better manage response procedures or "CONOPS" in case of a radiological event. Beyond better procedural response, IP Radiation Security tools can improve things such as forensic analysis, security policy, training and reporting. IPRS video systems can even automatically save video of an incident in a court-admissible format for evidentiary purposes.

There are three major categories of radiological security:

(1) Custodial—protecting materials in the places where they are used.

(2) Transport—monitoring the flow of goods and people to stop unwanted movement of illicit materials.

(3) Ingress—protecting potential target locations from a dirty bomb, or possibly the arrival of patients to a medical facility after a nuclear event.

For the purposes of this hearing on Radiological Source Protection, I have highlighted the application of these systems to Custodial activities. It should be noted that IP security tools could also be applied to Transport and Ingress applications. The waste management industry is one additional sector that can also use IPRS tools to help eliminate radioactive materials from transfer stations and landfills; again, not the focus of this statement of record.

The IAEA recently released publication number 1387, entitled Security of Radioactive Sources. It is an implementation guide for the security of facilities housing radiological sources that provides a comprehensive tool for legislators and regulators, physical protection specialists and facility and transport operators, as well as for law enforcement officers. (STI/PUB/1387, 66 pp.; 2009, ISBN 978–92–0–102609–5, English. Date of Issue: 6 July 2009.)

Below, I have enclosed Table 2 from IAEA's Security of Radioactive Sources publication, which outlines the specific objectives of a radiological security program, based on the prerequisite threat assessment that drives the prescribed security functions. This table identifies the many ways a fully integrated systems approach to radiation security can help to achieve the program recommended by the IAEA.

IPRS systems can be designed for a stand-alone facility, or to be incorporated into an enterprise security management software environment to maximize the scope of response capabilities. Systems can even enable communications that span across organizational boundaries. In all cases a threat assessment is conducted, and a security plan is developed, prior to systems design.

Below the IAEA's Table, I have taken the recommended security functions and measures presented in the IAEA guide and provided a lower level of detail to show how a range of commercial IP security systems, configured to work together with IP-enabled radiation instrumentation, can increase the likelihood of achieving the IAEA's stated security objectives.

TABLE 2.—SECURITY LEVELS AND SECURITY OBJECTIVES

	Security Objectives		
Security functions	Security Level A Goal: Prevent unauthorized removal [1]	Security Level B Goal: Minimize likelihood of unauthorized removal [1]	Security Level C Goal: Reduce likelihood of unauthorized removal [1]
Detect	Provide immediate detection of any unauthorized access to the secured area/source location		
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider	Provide detection of any attempted unauthorized removal of the source	Provide detection of unauthorized removal of the source
	Provide immediate assessment of detection		
	Provide immediate communication to response personnel		
	Provide a means to detect loss of source through verification		
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal	Provide delay to minimize the likelihood of unauthorized removal	Provide delay to reduce the likelihood of unauthorized removal
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal	Provide immediate initiation of response to interrupt the unauthorized removal	Implement appropriate action in the event of unauthorized removal of a source
Security management	Provide access controls to source location that effectively restrict access to authorized persons only		
	Ensure trustworthiness of authorized individuals		
	Identify and protect sensitive information		
	Provide a security plan		
	Ensure a capability to manage security events covered by security contingency plan (see the Definitions)		
	Establish security event reporting system		

[1] Achievement of these goals will also reduce the likelihood of a successful act of sabotage.

SYSTEMS AND THEIR CAPABILITIES

- Radiation Detection.—Alerts from "stand-off" IP sensors that sit on the security network and are strategically placed in a facility. These sensors can transmit the "activity" levels in terms of dose rate to first responders. These sensors give an indication of the strength of the source and "energy level," which helps to provide an indication of the isotope that has been detected. Software from Defentect in Norwalk, CT can gather specialized radiological data from many types of detectors from manufacturers like Ludlum Measurements, located in Sweetwater, TX, and transmit "intelligent" alerts to the other components of the security framework to help radiation safety personnel, security professionals, and public safety officials better understand the situation to which they are responding.

- Video Surveillance.—Video from cameras in the area that would capture a person's image and for storage in Digital Video Recorders. Robust video surveillance software addresses many other functions. Systems, like those from OnSSI of Pearl River, NY, enable customized viewing of many cameras, pushing of video to specified personnel on preset events, storage, and archival management of thousands of hours of recorded video, easy search interfaces to help security and radiation safety personnel investigate incidents, and saving of video in tamperproof court-admissible format. These systems offer "analytics," such as license plate recognition and specific detection rules for identifying suspicious activities.
- Access Control.—Authorized persons requiring access to a facility are required to provide information for use in conjunction with a magnetic swipe, or RFID card. Identity confirmation is made whenever the card (with PIN if required) is used to access a door in the facility. The database record created in the system can include the person's name, the door accessed and date/time of the attempt to access a doorway. This information can be combined with other elements of a comprehensive security management system.
- Interaction with a "tamper strap" device used to monitor the containment receptacles in which radiological materials are stored can trigger video surveillance, text messaging and calls for personnel to investigate the incident.
- Motion detection, a common feature of IP video surveillance management systems from companies such as OnSSI, triggers alerts to be generated to the system. Infrared sensors can also identify motion in a facility.
- Dry contact devices, which indicate that an analog electronic circuit has either been opened or closed. These enable a wide range of capabilities from identifying open windows to taking the pulse from an analog radiation detector. Equipment from companies like Defentect now exists to "digitize" the pulse from analog radiation instrumentation, so that the signal can be included into an IP radiation security system to enhance required security procedures.
- Systems can automatically generate instructions based on predetermined events to minimize injury, or loss of life. Documented response procedures, or CONOPS can be presented to responders in a variety of formats, so that they react to an event in the best possible fashion as outlined in planning and training.

Finally, all of these components must be configured to enable a faster, more informed response by police, fire, medical, and private security—in addition to management and regulatory officials. A security infrastructure must offer multifaceted communications and messaging between humans and machines. Examples of such communication ranked in order of response criticality include:

(1) Send relevant data to other components of the security system on the IP Network using a protocol called "XML."

(2) Broadcast video to guard stations, cars, handheld devices, cell phones, laptop computers.

(3) Send SMS text messages with incident details to responder cell phones and pagers.

(4) Send emails with incident details to personnel who need to be informed, but not necessarily respond immediately.

(5) Log all data (including video) to a database for later reporting, forensic analysis, training or policy analysis, and future personnel training.

With proper design and integration, mobile and wireless systems can also be supported to extend the security zone.

CONCLUSION

Certainly, terrorists have proven their capability to commit crimes against unsuspecting targets, making radiological security a bigger concern than ever before. While radioactive materials offer significant benefits to society and the vast majority is in well-secured environments, there are cases where responsible licensees have lost control of those sources. These cases represent only a small fraction of the total sources in use, but there have been a few cases of accidents, which have yielded serious consequences. Terrorism would make a radiation situation far worse and create serious consequences for civil society.

Vendors have begun to market COTS IPRS solutions that need broader consideration. A growing number of radiation control, physical and homeland security, and information technology professionals believe additional safeguards, including the networking of radiation detectors with IP-based security systems, is needed.

By including IPRS as part of an overall program that utilizes industry standard IP security and surveillance tools, users of radiological materials—and others concerned about securing facilities from threats posed by radioactive materials—can

implement radiation security and response systems on a broader and much more cost-effective basis than the proprietary systems deployed since 9/11.

IPRS is a natural extension of "digital convergence" in the disciplines of security and information technology. IPRS offers a reliable and cost-effective means to provide higher security for radiological materials. Security tools that are commercially available today can not only increase security, but also reduce start-up and operating costs in implementing large-scale source protection initiatives.

Thank you for the opportunity to submit this statement for the record. I am available to answer any questions you may have.

APPENDIX A.—NRC INCIDENT REPORT POST FROM IPRADIATIONSECURITY.COM BLOG

This is a case where IP radiation security systems would improve the understanding of what happened. Networked surveillance video and IP radiation sensors that work in concert with each other should have monitored the door and strategic internal locations. The video images and any radiation information (dose rate, count rate, energy level, isotope) could have been immediately transmitted to guard stations, corporate RSOs, local and State authorities, etc. as part of the standard response procedures in a comprehensive security plan.

General Information or Other	Event Number: 45301
Rep Org: GEORGIA RADIOACTIVE MATERIAL PGM Licensee: KAISER PERMANENTE Region: 1 City: JONESBORO State: GA County: CLAYTON License No.: GA1276–1 Agreement: Y Docket: NRC Notified By: ERIC JAMESON HQ OPS Officer: DAN LIVERMORE	Notification Date: 08/26/2009 Notification Time: 16:00 [ET] Event Date: 08/22/2009 Event Time: 07:30 [EDT] Last Update Date: 08/26/2009
Emergency Class: NON EMERGENCY 10 CFR Section: AGREEMENT STATE	Person (Organization): JOHN WHITE (R1DO) LANCE ENGLISH (ILTA) GREG SUBER (FSME)

Event Text

AGREEMENT STATE REPORT—EXTERIOR ACCESS DOOR TO RADIOLOGY LAB FOUND OPEN

While responding to an audible alarm, the Clayton County Police Department found an exterior door open to the Radiology Lab at the Kaiser Permanente Nuclear Medicine Clinic located in Jonesboro, Georgia. The Clayton County Police Department notified the Federal Bureau of Investigations and the Georgia Information Sharing and Analysis Center. The Georgia Information Sharing and Analysis Center then contacted the Georgia Radioactive Materials Program.

The licensee is authorized to possess diagnostic imaging isotopes. At this time, no information is available whether radiological material is missing, or if the open door was the cause of the alarm. The investigation is on-going.

* * * UPDATE FROM IRENE BENNETT TO JOHN KNOKE AT 1036 EDT ON 09/04/09 * * *

The State conducted an inspection at the licensee's facility and determined that no material was missing. A complete report will follow later.

Notified FSME (Angela McIntosh), R1DO (James Dwyer), and ILTAB (via e-mail).

These "Event Notification Reports" are posted to the NRC website for public review.

Ms. CLARKE. I would like to thank the witnesses for your valuable testimony and for your willingness to participate in today's hearing.

I would also like to thank the subcommittee Members that traveled to Brooklyn yesterday to participate, all the way from California. I hope you enjoyed your stay in our great borough, our great city, and our great State.

Members will have 10 days to submit questions for the record. Witnesses are reminded that Members may submit additional questions in writing, and we ask that you reply to the committee in writing in an expeditious manner.

Hearing no further business——

Mr. LUNGREN. Madame Chairwoman.

Ms. CLARKE. The gentleman from California.

Mr. LUNGREN. Before I respond to your inquiry about how we enjoyed this, can I say am I going to wait until I get my ride back to the train station before I can respond?

Ms. CLARKE. That will be fine, Mr. Lungren. See you in Washington.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 11:35 a.m., the subcommittee was adjourned.]

○