Statement for the Record

David Heyman
Assistant Secretary
Office of Policy
Department of Homeland Security

Before the
Subcommittee on Terrorism, Unconventional Threats and Capabilities
Committee on Armed Services
United States House of Representatives

July 28, 2009

Introduction

Chairman Smith, Ranking Member Miller, distinguished members of the Subcommittee: Good morning, thank you for the opportunity to address you today. My name is David Heyman. I am the Assistant Secretary for Policy at the Department of Homeland Security.

The topic of the hearing today is consequence management of chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) attacks. It is a topic that sits at the intersection of three winding roads: the spread of transnational terrorism, the proliferation of nuclear weapons, and the advancement and diffusion of biotechnology.

Today, Al Qaeda and its violent ideology have been reconstituted along the border region between Afghanistan and Pakistan. North Korea and Iran continue their steady pursuit of nuclear technology. And the capacity to manipulate, replicate, and manufacture genetic material—a capacity that has great benefit to society, but also in the wrong hands the potential for great harm—has now become widely available throughout the world.

Our top priority at the Department of Homeland Security is to secure the American people from a range of terrorist threats, and the prospect of these three roads coming together is of great concern to the Department. Preventing chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) attacks is at the core of DHS' mission and the reason the Department was created. So too is ensuring we are prepared for any attack that may occur, despite the nation's best efforts.

I am here today to provide you with an overview of consequence management at the Department for chemical, biological, radiological, nuclear and high-yield explosive (CBRNE) attacks, with an emphasis in biological and nuclear because they are particularly of high consequence Consequence management is a critical element in our nation's efforts to ensure that we are resilient in the face of an attack. We can be a more resilient nation, the more robust we are, the more agile we are responding to an attack, and the more rapidly we can recover. But, I should make clear from the start that we cannot talk about our ability to respond to and recover from an attack, to be resilient, without also simultaneously talking about prevention. Prevention and resiliency are two sides of the same coin—they are the yin and yang of our nation's risk abatement strategy.

Prevention and resiliency are both required to varying degrees as we consider combating CBRNE terrorist threats. In the case of nuclear attacks, the emphasis must be primarily on preventing an attack because the consequences of an attack would be catastrophic; for biological attacks, the emphasis must be on consequence management and ensuring resiliency because prevention is more difficult, and there are ways to save lives after an attack to prevent it from becoming catastrophic even after it occurs.

Regardless, whether we talk about prevention or resiliency, our goal is clear: we must put in place national—and in some cases international—systems of CBRNE defense, consisting of prevention, protection, response and recovery (or consequence management), that are robust, comprehensive, and resilient. This is not simply a DHS responsibility, though it is central to our mission. It is a national interest, requiring a comprehensive, integrated, and layered approach, combining the capabilities and resources of many entities across many levels of society: with the public, with State and local governments, across the Federal government and with our international partners, as well.

Prioritizing the CBRNE Threat

We can no longer discuss risk abatement of chemical, biological, and nuclear/radiological attacks as if these types of attack are unthinkable or undoable. U.S. intelligence, and the most recent intelligence around the world, continue to report that terrorists are intent on acquiring CBRNE

weapons for use against the United States.[1] While we have thankfully not seen a catastrophic CBRNE threat materialize, recent cases show the need for continued vigilance.

For example, from October 2006 to July 2007 insurgents in Iraq launched nearly 20 attacks using chlorine enhanced vehicle-borne improvised explosive devices (VBIED) that caused chlorine-related casualties including two fatalities. Kamel Bourgass – an al Qaeda-trained Algerian who had recipes and raw ingredients for making ricin, cyanide and botulinum with instructions on how to use these poisons and make explosives – was convicted of plotting to launch chemical and bomb attacks in London in 2005.

In Germany in 2007, four men known as the "Sauerland Cell" were found to have purchased enough bomb-making materials, including hydrogen peroxide-based liquid explosives, that could build bombs more powerful than those used in the 7/7 London bombings and the 3/11 Madrid attacks. In Maryland in 2005, Myron Tereshchuk was convicted of possessing weaponized ricin. The 2001 anthrax attacks in the U.S. mail, including in letters addressed to two United States Senators, were of the most significant biological events we have seen, especially here at the Capitol; five Americans died in these attacks.

Nuclear and radiological materials, including fissile material for nuclear weapons, remain very possible to acquire. In January, 2004, Abdul Qadir Kahn, a Pakistani nuclear scientist, confessed to running a vast clandestine supply network of nuclear weapons secrets and technologies; Iran, Libya and North Korea were the recipients. A thriving black market exists for radioactive materials, including fissile materials suitable for nuclear weapons. The International Atomic Energy Agency reports that "from January 1993 to December 2006, a total of 275 incidents involving unauthorized possession and related criminal activities were confirmed to the Agency's Illicit Trafficking Database."

DHS continually applies this understanding to domestic prevention, protection and response planning. The DHS Science and Technology Directorate (S&T) produces a biennial Bioterrorism Risk Assessment (2006, 2008), a Chemical Terrorism Risk Assessment (2008), and – in partnership with the DHS Domestic Nuclear Detection Office (DNDO) – an integrated CBRN Risk Assessment. Continuous risk assessments from all-source intelligence are performed by our

[1] Dennis Blair, Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, U.S. Senate,* February 12, 2009.

DHS Office of Intelligence & Analysis (I&A) in collaboration with our six component members of the DHS Intelligence Enterprise and the entire Intelligence Community. These risk assessments, together with current intelligence, guide the policy priorities and point to our greatest opportunities for risk abatement in the various attack scenarios.

What I am going to talk about today is DHS's CBRNE risk mitigation, with a focus on DHS' role in consequence management. Nuclear and certain types of biological attacks are the most serious threats we face – not because they are necessarily imminent, but largely because of the potential catastrophic impact or consequences an attack would have. Beyond the cost to human life, a successful nuclear or catastrophic biological attack would have far-reaching physical, economic, and psychological impacts.

The Role of DHS

As Secretary Napolitano has said, one of our principal priorities within the Department's all-hazards mission is to ensure that the Nation can respond to and recover from an incident such as a terrorist attack. Specifically, the Homeland Security Act of 2002 tasks DHS with "developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to chemical, biological, radiological, nuclear and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts."

A number of National Security and Homeland Security Presidential Directives (NSPD/HSPD) further define the Department's role and responsibilities for holistic risk abatement of CBRNE threats:

HSPD-4 National Strategy to Combat Weapons of Mass Destruction
HSPD-5 Management of Domestic Incidents
HSDP-8 National Preparedness
HSPD-9 Defense of the United States Food and Agriculture
HSPD-10: National Strategy for Biodefense in the 21st Century
HSPD-14 Domestic Nuclear Detection
HSPD-15 U.S. Strategy and Policy in the War on Terror, CBRNE chapter

HSPD-19 Combating Terrorist Use of Explosives in the United States
HSPD-22 Domestic Chemical Defense

For consequence management, of particular importance is HSPD-5, Management of Domestic Incidents. The purpose of HSPD-5 is "to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system." HSPD-5 gives the DHS Secretary incident management oversight authority and directs the Secretary to develop a National Response Plan (now called the National Response Framework) to integrate Federal Government domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan, including CBRNE incidents. Additional legislative authorities for DHS reside in the SAFE Ports Act and the Post-Katrina Emergency Management Reform Act of 2006 (PKEMRA).

Preventing and Responding to a Nuclear Attack

Preventing and responding to a nuclear attack involves a multi-layer strategy. The Nation's first line of defense against a nuclear attack is to control the sources of material and proliferation of nuclear technologies in order to prevent a nuclear attack. To thwart proliferation, overseas programs, such as the DoD Cooperative Threat Reduction Program and DOE's Second Line of Defense Program, strengthen the capability of foreign governments to secure, dismantle, deter, detect, and/or interdict illicit trafficking of nuclear and radioactive materials across international borders and through the global maritime shipping system.

If material can not be controlled at its source, the next layer is to detect its movement from where it was taken to its eventual target. DHS has a statutory responsibility to develop a Global Nuclear Detection Architecture (GNDA). The GNDA is a multi-layered system of programs, guidelines and detection technologies operated by federal agencies and designed to enhance the nation's ability to detect and prevent a radiological or nuclear attack. The Department of Defense, Department of Energy, State Department and other Federal agencies play key roles in this important effort.

DHS also coordinates with the Department of Energy on the Megaports Initiative, which equips foreign partners with radiation detection equipment at their sea ports. Approximately 75 ports worldwide are targeted for implementation of the Megaports Initiative. In addition, the Secure Freight Initiative (SFI) builds on the successful efforts of the DHS Container Security Initiative

(CSI) and Megaports programs by using the latest available technology to identify containers that pose a risk to the global maritime supply chain.

If radiological materials or nuclear weapons make it out of port, the Proliferation Security Initiative (PSI) enables the interdiction of illicit shipping of CBRNE materials on the high seas. The State Department credits PSI with halting 11 CBRNE-related transfers from 2004 to 2005, and more than two dozen from 2005 to 2006. Just this past June the United States Navy trailed a North Korean vessel suspected of moving materials that could be used to make a CBRNE weapon. We are also focusing efforts on other avenues of entry into the US, including general aviation, small maritime vessels, and non-points of entry land borders. Within the U.S. we will soon conclude the Securing the Cities Initiative, a pilot program to detect radiological or nuclear materials entering key urban areas such as New York City. Our operational components, such as U.S. Customs and Border Patrol, the Transportation Security Administration, and the U.S. Coast Guard are helping prevent nuclear terrorism every day.

Today I have been asked to testify on the last line of defense. Should other defenses fail, DHS, and its partners, must be ready to respond. It is DHS doctrine to take an all-hazards approach to response. Just like natural disasters, a terrorist nuclear attack would be handled by the primary response arm of DHS, the Federal Emergency Management Administration (FEMA). FEMA has been responding to disasters for over 30 years, and with the empowerment of the Robert T. Stafford Disaster Relief and Emergency Assistance Act as amended (Stafford Act), FEMA, with a Presidential declaration, has the ability to assist State and local officials in disaster-stricken areas. The White House, with substantial input and support from DHS, recently released Planning Guidance for Response to a Nuclear Detonation. This guidance is aimed at assisting State and local planners in preparing to respond to a nuclear attack, but also guides Federal planning. Not withstanding the guidance, a nuclear attack against the homeland would pose an extraordinary challenge, one that the Department is working diligently to meet. DHS values its strong and close working relationship with the Department of Defense (DoD) in all-hazards disaster response activities. In addition, FEMA is collaborating with DoD and others to develop a Strategy to Improve the Nation's Response and Recovery from an Improvised Nuclear Device (IND) Attack. FEMA will take the lead for DHS in coordinating with our federal partners to ensure our nation's ability to support state and local needs in the event of a nuclear attack. The program is currently funded at $6 million in FY09.

The first mission objective in response is to save lives, and all our planning emphasizes the preeminence of life-saving. Research and analysis on sheltering options shows that proper preparedness can save many lives during an incident involving highly radioactive fallout. Nuclear fallout is extremely radioactive in the first 2 hours post-detonation, but decays away fairly rapidly. Effectively sheltering people during those early hours can save tens of thousands of lives. With effective public outreach, local preparedness, and timely communication, we can save many lives. This is an area we continue to research and incorporate into plans. The DHS Office of Health Affairs produced a science-based public communications guide to assist Federal, State and local officials in preserving life following a nuclear attack. FEMA National preparedness, working with the DHS Office of Health Affairs, is now developing the communications tools for use by the State and local community to educate the public about IND events and to provide accurate protective action instructions in the minutes and hours after an event.

Preventing and Responding to a Biological Attack

Unlike radiological or nuclear threats, we face a much different set of challenges with respect to biological threats. It is difficult to counter a surreptitious release; there are more than 30 unique biological threat agents and various deployment scenarios. We are in the midst of a global biotechnology revolution and the skill set to manipulate pathogens is ubiquitous and rapidly advancing. New discoveries in the life sciences point to possible cures for cancer; at the same time, new research could be misused for deadly effect.

The biggest building blocks of the Nation's biodefense strategy are: (1) to detect-to-treat – DHS operates the BioWatch program for early recognition that a bioattack has taken place, (2) the development through HHS and DOD of medical countermeasures to protect people from the attack, (3) the partnership between DHS and National Center for Medical Intelligence (NCMI), and (4) strengthening the public health community at the State and Local level to effectively treat the exposed population to mitigate illness and death. Because of the potential mass scale of an attack, the integrated Federal biodefense experts are focused on developing surge capacity and taking measures to drive the timeline for response as early as possible.

DHS funds the national BioWatch program and supports the daily operations of existing technologies that test and analyze air samples for the presence of biological agents. DHS also

funds the development of next-generation of biodetection technology that aims to shorten warning times to four to six hours of an attack. Fielding the next generation systems includes overcoming challenging technological and engineering hurdles and must be fully tested before being deployed. Because clinical symptoms may not show up in victims for many days after an attack, the BioWatch detection systems form a critical part of enabling a rapid response to mitigate illness and death. The BioWatch program is part of an integrated Federal partnership that includes the HHS distribution of the strategic national stockpile to a location, and the dispensing of post-exposure prophylaxis by Federal, State and local officials to the affected population. DHS, HHS and DOD also partner together to maximize investment utility on medical countermeasure development and acquisition for the most relevant vaccines and drugs, and jointly establish R&D priorities to respond to a full range of bio and chemical threat agents.

Further DHS layers of defense against biological threats include building awareness at home and abroad. We seek to prevent the deliberate misuse of biologic agents and we assess the deliberate adversary threat when powerful new biotechnologies are discovered. We support international engagement with other countries, the international private sector, and the global public health community to build awareness, understanding, and responsible conduct. DHS also knows that investments in public health against infectious diseases can contribute to public health security in the United States, which is why we maintain a robust risk assessment to understand the relative risk posed by various biological agents, and provide the national priorities for countering the greatest threat: an aerosolized release in a major urban area.

Adding protection against security or safety lapses, and insider threats forms another layer of biodefense. DHS supports site vulnerability assessments on behalf of the select agent research community at Biological Safety laboratories. Pathogens reside in 300+ research sites throughout the U.S. and in multiple countries around the world. Sufficient biological security measures need to be put in place and intelligence collection strengthened to prevent unauthorized access to these pathogens. DHS is a leader in people screening, particularly screening those with ties to terrorism and international connections. DHS builds on our resources within TSA, CBP, ICE, I&A, Coast Guard and US-VISIT to enhance screening techniques, terror watchlist analysis, biometric collection, and cooperation with international partners. All these efforts help us limit the movements of those who intend to do us harm, which contributes to our prevention mission.

There are windows of opportunity to prevent a biological attack from becoming a catastrophic event. Timely mitigation measures, such as preparing citizens in advance for rapid delivery of post-exposure prophylactic medical countermeasures, are critical. Depending on the nature of the biological threat – even 2009-H1N1 – DHS works diligently on developing preparedness and response doctrine, exercises, training and public health and medical readiness, with a particular focus on leading preparedness and response activities with the private sector, critical infrastructure, law enforcement, first responder and other sectors not part of the traditional public health community.

Should a catastrophic bioevent happen, DHS must be ready to respond along with HHS, DOD, EPA and the State and Local public health communities. Biological attack scenarios are amongst the most challenging we may face and we are working to meet those challenges. We value our strong and growing relationship with the Department of Defense in this area for collaboration. A biological attack scenario would require a massive surge in manpower and resources to effectively save lives and manage the incident; DOD has manpower and resources that could be employed in this situation. .

Surge Capacity and Interagency Coordination

Surge capacity is vital to effective consequence management of large-scale CBRNE events. The national architecture for responding to a CBRNE incident, both natural and man-made, assumes first and foremost a local response, with individuals and local communities managing and coping with the initial stages of an incident. When an incident occurs that exceeds or is anticipated to exceed local or State resources, a surge of additional resources and capabilities is required. Those resources may come from nearby states or from the Federal Government. For major disasters, as governed by the Stafford Act, this surge can be initiated through the request of a State Governor for regional and/or Federal support. It can also be initiated by Presidential declaration.

It is anticipated that large-scale CBRNE events are likely to overwhelm State and local capabilities, quickly requiring additional resources from the Federal Government. Thus, DHS is actively working to further develop two key roles in CBRNE response preparedness: (1) to assist state and local responder organizations in preparing to recognize and respond to the novel or unique aspects of CBRNE attack, and (2) to coordinate the Federal response. Assistance to State and local stakeholders is largely provided through grants to state and local governments from FEMA, State and local outreach efforts, exercises, and training; In FY2009 DHS announced over

$1 billion in homeland security grants to States and local governments to build and strengthen preparedness capabilities through planning, equipment and readiness for all hazards, including CBRNE preparedness. As required by HSPD-8 and PKEMRA, FEMA also provides assistance by establishing readiness metrics in the National Preparedness Goal to measure national progress as well as an overall National Preparedness System for assessing the nation's preparedness capability to counteract CBRNE threats. Additionally, FEMA develops preparedness guidance to support the enhancement of these capabilities. FEMA also manages a Pre-Positioned Equipment Program that has caches of hazardous materials response equipment located at nine sites across the country to support state and local first responders in the event of a CBRNE attack or other disasters involving hazardous materials.

DHS interacts daily with Federal counterparts to ensure maximum coordination on issues such as CBRNE threats and intelligence, public health issues, infrastructure protection and security, counterterrorism and counterproliferation, secure transportation and shipping, and disaster response coordination. DoD, and in particular, NORTHCOM play major roles in many of these areas. We value our growing collaboration with NORTHCOM on the coordination, utilization, and integration of DoD assets and capabilities into Federal, State and local disaster response. The consequences of a nuclear attack are of such magnitude that civilian response forces would be unable to meet the demand. The massive surge in capabilities required to effectively save lives and manage the incident would require DoD manpower and resources in terms of specialized CBRNE hazard response teams, search and rescue capabilities, road clearing, engineering support, airlift for emergency evacuations and delivery of supplies, emergency medical care and supplies, shelter for displaced populace, provision of food and potable water, and other critical services.

DHS places a high priority on stakeholder outreach and engagement. One such example is the Interagency Biological Restoration Demonstration Program (IBRD), a collaborative Department of Homeland Security and Department of Defense program focused on reducing the time and resources required to recover and restore wide urban areas, military installations, and other critical infrastructure following a biological incident. The pilot city for IBRD is the Seattle Urban Area which includes Army Fort Lewis and McChord Air Force Base. The IBRD program is developing and demonstrating technologies and methods for wide area bio-restoration, and providing consequence management guidance at the local, state and federal levels.

Conclusion

Our nation faces many challenges with respect to CBRNE defense. Our top priority will always be to mitigate the risk in the best way possible which includes robust planning and preparedness. For nuclear threats, we will continue to focus on prevention; and for biological threats, the emphasis is on tight and timely response. Prevention and consequence management in CBRNE is a priority for the Administration and one that requires continued collaboration with our Federal, State, and local partners. We look forward to strengthening our existing partnership with the Department of Defense as we improve our Nation's resilience.

I would like to thank the committee for their support as DHS carries out necessary steps in the areas of preparedness, outreach to State and local governments and first responder communities, research and development, and planning for CBRNE prevention and consequence management. Thank you and I look forward to your questions.