Statement of Dr. Richard L. Wagner, Jr.

Chair, Defense Science Board Task Force on Prevention of,
and Defense Against, Clandestine Nuclear Attack
and
Senior Staff Member, Los Alamos National Laboratory

before the

House Committee on Homeland Security:
Subcommittee on Prevention of Nuclear and Biological Attack and Subcommittee on Emergency Preparedness, Science, and Technology

at their hearings on

"Detecting Nuclear Weapons and Radiological Materials: How Effective Is Available Technology?"

Tuesday, June 21, 2005

Statement of Dr. Richard L. Wagner, Jr.

Mr. Chairman, Mr. Chairman, members of the committees, I am honored to be here to speak to you about the effectiveness of available technology for detecting nuclear weapons and radiological materials, and the potential for improving effectiveness in the future with new technology resulting from research and development. I am encouraged that the House Committee on Homeland Security and its subcommittees have focused so strongly on the crucial task of protecting our nation against clandestine nuclear attack.

I represent the 2002/2003 Defense Science Board Task Force on Prevention of, and Defense Against, Clandestine Nuclear Attack. I am a senior staff member with the Los Alamos National Laboratory, although I do not represent the laboratory here today.

Nearly forty-five years ago, my Ph.D. thesis experiment in physics involved radiation detection. Since then, on several occasions, I have done additional scientific work, or managed programs, that involved advanced radiation detection. Over thirty years ago, I helped form, at the national laboratories, what later became the DOE's Nuclear Emergency Search Team (NEST). In the winter of 1978, I was co-scientific-leader of the NEST deployment to northern Canada to search for radioactive debris from the Soviet Union's Cosmos 954 satellite. In the 1980s, as Assistant to the Secretary of Defense for Atomic Energy, I brought NEST capabilities into the Department of Defense, and was involved in various activities to detect nuclear weapons. In 1997, and again in 2002/2003, I chaired Defense Science Board (DSB) Task Forces related to defense against smuggled nuclear weapons.

I want to make the following six points to you today:

1. Radiation detection at portals is but one part of what must be a multilayered, multi-component, civil/military, global architecture to prevent smuggling of nuclear weapons into the US. Effective detection at portals will require detection of other signatures than radiation, but effective radiation detection is essential.

2. Currently installed radiation detection systems, or systems which could be procured in quantity in the next year or two, are quite limited in their capabilities and, in general, are insufficient to the task. Substantial research and development (R&D) is needed to improve detection capabilities. But deployment of even the limited near-term capabilities should be significantly expanded to: 1) provide some degree of added protection for the nation in the near term, 2) expand the experience base in operations with radiation detection systems in order to help guide research and development of greatly improved capabilities for the future, and 3) build the necessary industrial base.

- When I speak of radiation detection capabilities, I mean not only the detectors themselves, but networks of detectors, communications and signal processing, protocols for resolving alarms, and operational concepts for detection and response-to-detection systems.

3. With an expanded, spiral, research and development (R&D) program, carried out in the aggressive style that characterized certain highly successful R&D programs in other areas over the past few decades, capabilities to detect the presence or transit of nuclear weapons can be improved greatly, within about five years, before reaching the limits imposed by the physics involved.

- Capabilities of specific detectors against specific weapon designs are classified. Appendix #1 is an unclassified excerpt from the report of the most recent DSB Task Force that I chaired, which describes in general terms current and potential future detection capabilities.

4. I cannot provide you with a detailed prescription for how to apportion resources, over time, among near-term deployments with limited capability, R&D, and later deployments of improved capability. Such time-phasing must be worked out in some detail, and must be allowed to change flexibly, even within budget cycles, as operational experience is gained and as early results of R&D come in. But it might be useful for you to think in terms of four generations of capabilities, as follows:

- Currently installed detection systems.
- Modest but worthwhile improvements that might be developed and deployed within a year or two.
- A first generation of greatly improved detection systems that would be quite expensive, but which should nevertheless be deployed in limited quantities to protect some crucial locations and to try them out in the field.
- A generation that achieves greatly improved detection at greatly reduced cost, which would be widely deployed in the mature, objective architecture.

5. Even with the best detection systems, the overall future protection architecture will not be perfect. No defense can be perfect. But a less-than-perfect defense can be effective if it has enough capability to:

- Cause prospective attackers to have serious doubts as to whether they will succeed.
- Create synergies with other system elements, for example by forcing the attacker to mount a larger operation which is more likely to be discovered so that warning can allow the defense to surge its capability.

I believe that, with an aggressive R&D program, we can achieve that level of capability. The utility of a less than perfect defense is discussed in Appendix #2, which is also excerpted from the DSB report.

6. The establishment, by the administration, of the Domestic Nuclear Detection Office (DNDO) is a big step in the right direction. It should be strongly supported by the Congress, along with especially strong support for “transformational R&D”. But work on transformational capabilities is unlikely to be effective unless it is carried out in the style that characterized certain highly successful R&D programs in other areas over the past several decades. In Appendix #3, which is

derived from recent discussions on this subject among me and a few broadly experienced colleagues, I mention these programs and say some things about their style. Support of the Congress will be essential in doing the program this way.

APPENDIX #1. EXCERPT FROM DEFENSE SCIENCE BOARD REPORT:

4.0 ASSESSING DEFENSE PERFORMANCE AND THE UTILITY OF POTENTIAL SYSTEMS' IMPROVEMENTS

……..Defense performance is determined by many factors. The performance of radiation detection systems is only one of them, but it is an important one, and we will use such systems' performance to illustrate broader issues.

As with other elements of the protection/prevention architecture, the performance of radiation-based detection systems can be thought of on three levels. ……

At the level of detailed technical metrics—detection range, detection time, false alarm rates, etc.—much of what this report recommends is based on our judgment that significant improvement is possible in detection-systems' performance in threat scenarios. Relative effectiveness is not too difficult to assess, but assessing absolute effectiveness is difficult for several significant reasons. One difficulty is that the utility of detectors in real operations depends strongly on natural radiation backgrounds, which vary greatly from place to place and often in time. Such backgrounds, and the nature of radiation detection in general, introduce a probabilistic element in assessment of performance, and the significance of detection and false-alarm probabilities is very scenario-dependent. All of this fuzzes concreteness, which creates difficulties in assessing system performance and in planning defense (and is one basis for our belief that performance can only be determined by field experience with real systems)……

4.1 Radiation detection performance

Despite these difficulties, rough estimates of radiation detection performance can be made. The referenced IEEE paper lays out some approaches to improving radiation detection and attempts to assess the degree of improvement in terms of both technical metrics and scenario assessment. Key points are excerpted below.

Today's capabilities. Only passive detection is available today. Correlated operation of multiple detectors can be done today only for a small number of sensors that can be integrated by human intelligence, assisted by limited automatic processing. With these and other capabilities:

- Plutonium devices can be detected in vehicles at portals, in cargo containers, and in vehicles at speed, if the device is unshielded or lightly shielded.
- Detection of devices containing highly enriched uranium (HEU) is very difficult and varies widely and is limited today to short range. In some cases lightly shielded devices can be detected at portals. In other cases they can be detected only if they are essentially unshielded.

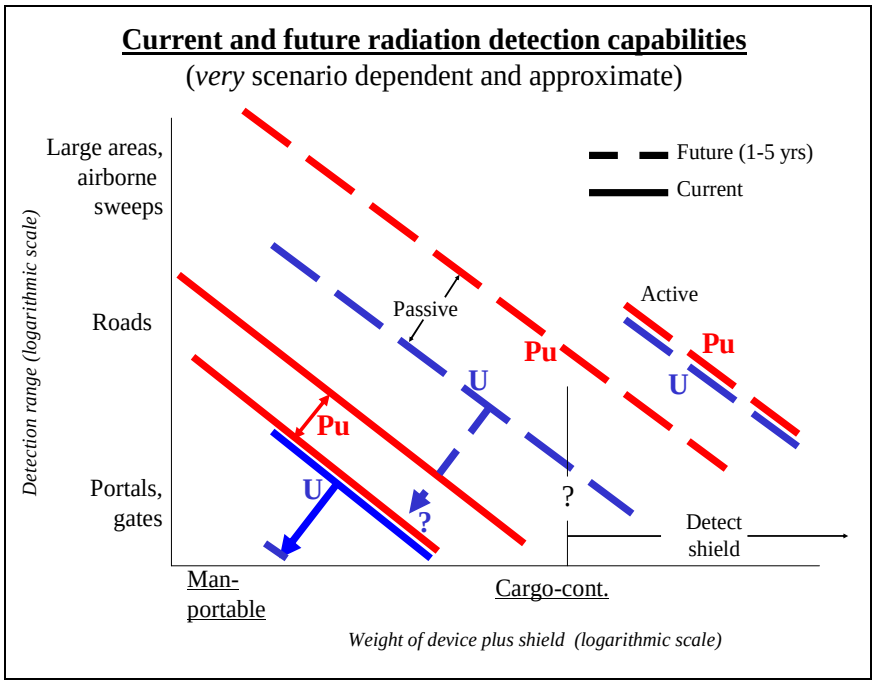
Some high-value targets are defensible, thanks to geographic features that channel traffic through defensible chokepoints, where capable portal monitors can be stationed. Traffic that attempts to bypass these chokepoints (e.g., on foot) is by definition suspect, and can be detected by non-nuclear techniques.

These current capabilities may be impaired by high and/or variable natural radiation backgrounds or innocent man-made radiation sources that yield unmanageable false alarm rates.

In the future. This report recommends greatly expanded R&D on radiation detection. The referenced IEEE paper illustrates some improvements in capabilities that would result from R&D. The following points summarize the potential benefits:

- Detection range can be extended by an order of magnitude, opening new defense operational modes such as rapid, wide-area airborne and vehicle sweeps, and monitoring large remote areas and/or extensive road networks. Shielding around the weapon could reduce performance of the detection systems, but the shielding mass can slow down the attacker and expose him to discovery by other means—e.g., detection of the shielding itself.
- Increased range and improved false alarm rejection will enable intelligent networking of detectors. This could enable coverage of road and rail transport over significant distances—e.g., along the U.S. East Coast, where long-distance transport must pass through a relatively small number of choke points.
- Background and innocent alarm rejection will allow detection of HEU in a wider range of circumstances, for example (in certain cases) in cargo that is naturally radioactive (e.g., bananas).
- Increased sensitivity and background rejection could virtually eliminate the effects of *incidental* shielding in vehicles or cargo containers, except for HEU in certain cases.
- More-portable and longer-lived sources for active interrogation will enable widespread screening of containers and vehicles. Advances in detectors and sources will allow operational restrictions on active interrogation due to health and safety concerns to be reduced.

Beyond such general and qualitative statements, what can be done with radiation detection is complicated to describe. It is a multi-dimensional parameter space, even for a single attack scenario against a single defense layer. There are many possible scenarios, and we have posited a multi-layer defense. The format of the chart below is one greatly simplified way of summarizing some of this complexity. It illustrates a fundamental offense/defense trade between the detection range and time available for detection, and amount of shielding around the device that can reduce the radiation output of the threat object.



The detection metric that the vertical axis represents is a function of range and dwell-time, and it varies by approximately six orders of magnitude along that axis. The diagonal lines on the chart reflect current and future capabilities, some of which are summarized in the paragraphs immediately preceding the chart. The uncertainties and variations in the vertical location of the diagonal lines are about an order of magnitude, as illustrated by the plutonium current technology line. The relative locations of the lines are less uncertain. ……..

Appendix #2: Excerpt from Defense Science Board Report

4.3 Thinking about the utility of imperfect defenses

When and if the community involved in this work becomes able to assess system performance against threats accurately and comprehensively, it will be found that the defense is not leak-proof, as no defense can be. Because of this, some might argue that devoting the level of resources entailed in the Task Force recommendations would be wasted. We believe this is profoundly wrong. No protection system can be perfect, but over the course of history, defenses that are far from perfect have played vital strategic roles. To deal analytically with the issue of imperfect defense, the third level of performance measures—including the overall goals of the defense—must be addressed……..

With the best technology we can develop, how effective can prevention/defense be?

- Much better technology is essential, but not sufficient alone
- Right goal -- not perfection; rather: attenuate threat, dissuade attempts, thwart some attacks, delay successful attack
  - Historically, imperfect defenses often effective
- Reference point: during late '70s, early '80s, the US……
- Best technology can raise defenses above "the threshold of dauntingness", dissuade attempts.
  - Deliberately create uncertainties for attacker
- Synergies help. Examples:
  - Better defense → larger threat operation → more signatures → possible warning → surge defenses
  - Concentrate nuc mat'ls control on hardest-to-detect mat'ls
- Can't answer with paper studies; can find out only by trying

The stakes are worth the bet.

6

The goal that should be set for a national/global system and its DoD elements is not perfection. Rather, because clandestine nuclear attack attempts will not be frequent, the goal should be to substantially attenuate the frequency of successful attacks (including significantly delaying the first one). Delay and attenuation could provide time to mitigate the threat in other ways, including measures to ameliorate the underlying political and cultural factors that stimulate the terrorist threat, writ large.

Many of us believe that a strong case can be made that prevention/protection can be developed that will substantially attenuate the frequency of successful attacks, by being good enough to (1) dissuade or deter many of those who might consider attempting attacks and (2) thwart or defeat a good fraction of the (fewer) attacks that might be attempted. The deterrent aspect of the protection equation involves the often-great differences between how a defender and an attacker will view the relative capabilities of the defense. The long history of offense/ defense competitions is strongly characterized by both sides taking own-side-conservative views. More particularly, the annals of terrorism and counterterrorism are replete with instances in which a prospective attacker was deterred by aspects of the defense that may have seemed relatively weak and ineffectual to the defender. The terrorist may not be afraid to die, but he (or his master) does not want to fail

Dissuasion/deterrence by the adversary's fear of failure might work in a variety of ways. One aspect is that an attacker will want to know enough about the defense to design a robust, successful attack. If the capabilities of the defense can be improved enough that the attacker must know the details of defensive measures in place to understand how to best surmount them, then the attacker may expose himself to discovery during the planning phases of the attack or be altogether dissuaded from the attempt.

Creating uncertainty in the attacker's mind will be critical to maximizing the success of defenses which, realistically, cannot aspire to perfection. To exploit the effects of uncertainty, the defense should be deliberately designed and deployed to create as much ambiguity for the attacker as

possible as to where the "boundaries" of defense performance lie. Deliberate deception should be used (carefully) as part of an overall perception management effort.

Data that can be used to be more analytic about these and other deterrence effects should be systematically assembled from the annals of counterterrorism.

Many kinds of synergies contribute to defense effectiveness. An obvious one is the effect of a layered defense, as we propose. With multiple layers, each layer need not be highly effective in order for the overall effectiveness to be high. If the layers require different tactics or technologies to penetrate, the attacker's job is considerably more difficult. This indicates a fundamental synergy between a layered defense and the capability to detect the threat by intelligence indicators, including from law-enforcement activities. A more capable and varied defense means that the attacker must mount a larger operation to penetrate it. A larger operation has more (and more observable) signatures. More people with more skills must be recruited and trained; more money must be obtained and laundered; the operation takes longer; and the attacker must surveil the defense more intensively. By increasing the signature of attack planning, the likelihood of discovery increases commensurately. This, in turn, could allow the defenses to be surged, further increasing effectiveness.

These preliminary thoughts about the effectiveness of a defense have led the Task Force and its predecessors to become convinced that reasonable success in mitigating the threat is sufficiently likely that, in light of the seriousness of the threat and of the consequences of successful attack, a serious development and deployment program is warranted..

Appendix #3: Assuring program effectiveness

The establishment of the Domestic Nuclear Detection Office (DNDO) is an extremely positive step in improving and deploying detection systems, and will provide a group which, adequately funded and properly located organizationally, can do much to accomplish the objectives cited above. But in light of the stakes involved, it is fair to ask whether DNDO will be able to improve deployed detection technology as much and as quickly as possible. DNDO's charter and authorities, as they are expressed in its founding documents, are sound as far as they go, but there are intangibles that are crucially important for success and that are difficult to address in a charter or authority. These intangibles are what I address here.

To deal with such a difficult scientific, technological, and operational issue requires innovation, free thinking, continuity of effort, creativity and simultaneous risk taking (technology investments that may ultimately prove dead-ended). None of these qualities are among those generally attributed to the government's conventional research and development process—which often discourages even prudent risk taking and is at best ponderously slow.

It has generally been found that truly creative research is best pursued by maintaining close coupling between the researchers and those dealing with day-to-day operational challenges. At the same time, it is exactly these latter challenges which often usurp the attention, priority, and budgetary resources which would otherwise be devoted to longer-term research.

When facing such challenges in the past the government has generally been most successful when it removed the attack on a specific high priority problem from the every-day research and development process and established a dedicated, high priority assault on the specific issue at

hand. DNDO is intended to catalyze such an assault, but whether it will be successful will depend on its ability to emulate key features of past successes. Examples include the Manhattan Project, the Apollo Project, the development of the Polaris submarine system, and the development of the U-2, SR-71 and F-117 at the "Skunk Works". What is needed is a mini-Manhattan Project which focuses specifically on the detection of nuclear weapons and materials. The development of a weapons detection capability is not an easy task, but neither was the development of the nuclear weapon itself.

Key features of many of the past successes mentioned above include:

- high-risk, high-payoff developments are pursued, hedging against possible failure with alternative approaches carried out in parallel;
- R&D reaches from basic research through to fieldable prototypes;
- a streamlined management process with minimal "outside" influence;
- a cooperative and open relationship between government and industrial/academic participants;
- the role of senior, centralized government leadership is to set broad goals, secure funding, and provide freedom of action for the R&D teams; and
- the R&D is conducted mainly outside of government by large, integrated, multi-disciplinary R&D teams with forceful and experienced leaders, and with:
    - wide latitude to achieve broad, ambitious, mission-level goals,
    - direct, frequent, working-level contact between users and R&D people,
    - freedom to change R&D objectives and approaches quickly and flexibly as the R&D proves what is feasible, and
    - the expectation of continued involvement to achieve both near-term milestones and long-term goals.

To accomplish such a feat would entail waiving many of the existing procurement regulations which were designed to conduct the ordinary course of research and development in the government.

The approach sketched here would be exceptional today – a significant departure from the way most government R&D is currently done. Because of this, it will be controversial and difficult to implement and will need high level support, including from the Congress.