HEARING ON
"BUILDING A NUCLEAR BOMB:
IDENTIFYING EARLY WARNING INDICATORS OF TERRORIST ACTIVITIES"
BEFORE THE SUB-COMMITTEE ON
PREVENTION OF NUCLEAR AND BIOLOGICAL ATTACK,
COMMITTEE ON HOMELAND SECURITY,
U.S. HOUSE OF REPRESENTATIVES
May 25, 2005
1:00 PM, CANNON HOB 210

STATEMENT
BY
THE HONORABLE RONALD F. LEHMAN
ON
TERRORIST ACCESS TO TECHNOLOGY AND TECHNOLOGISTS

Mr. Chairman, Distinguished Members of the Committee;

I am honored that you have asked me to join in your examination of the danger of nuclear terrorism. As this Committee knows, I have assisted the US government in a number of areas that relate to this topic and continue to do so. Both personally and professionally, I consider these initiatives to be very important, but you have asked for my personal views. Thus, today I do not speak officially for any program, organization, or Administration with which I have been or am now associated.

Much has been said in public about nuclear terrorism, not all of it correct. And that is not all bad. Indeed, special care must be taken not to provide terrorists with "cookbooks" to solve their problems. Nor do we want to expose to them vulnerabilities they might exploit or reveal too much about countermeasures we may be able to take. Above all, we must be candid with ourselves. There is much that we don't know or may not find out until it is too late, particularly about specific terrorist planning and activities. We will be asking constantly whether the glimmers we see are the "tip of an iceberg" or simply disconnected "ice cubes."

Although the odds that any particular group of terrorists will acquire nuclear weapons are low, the probability that some terrorists somewhere will acquire a nuclear weapon may increase over time. The consequences could be tragically high. We must take the possibility of nuclear terrorism very seriously now and in the years ahead as relevant technologies continue to spread, no matter how difficult we make it for terrorists to acquire nuclear weapons. This requires that publics be sensitive to the danger, particularly those who may someday find themselves in a position to help. Thus, we must balance not saying too much with saying enough.

You have asked me to focus today on the possibility that terrorists might gain access to technology and technologists useful to the acquisition of nuclear weapons. Here, we understand basic realities and a number of trends. Building nuclear weapons from scratch is a challenge.

Terrorists may find it easier to obtain them by theft, gift, or purchase from sympathetic governments or rogue government organizations. Even this will not be easy, and the U.S. and other governments have programs and policies aimed at preventing just such activities. Particularly with the help of sufficiently knowledgeable "insiders," however, fissile material, key weapons components, or full-up nuclear weapons could be purloined. Much has been made of inadequate security in the transition republics of the former Soviet Union. South and East Asia also deserve special attention, but securing fissile material remains a global problem.

Still, we cannot rule out the possibility that terrorist organizations may attempt to assemble nuclear weapons from components or even from amounts of fissile material obtained from some source. (It is unlikely that typical terrorist groups would by themselves succeed in enrichment or reprocessing, but it is conceivable.) Although assembly may be a far more difficult path than theft, considerable knowledge and technology including dual-use equipment and facilities once associated with nuclear weapons continues to become more accessible. And whether nuclear power generation expands or contracts in the years ahead, a huge overhang of weapons-useable material will remain as a potential source of nuclear weapons even if no new production were to take place and even if we eliminate large amounts of existing fissile material.

In that sense, we already have strategic warning. We know there is great risk. We can point to general indicators such as the spread around the world of dual-use scientific knowledge, engineering skills, industrial capabilities, nuclear materials, and the like. A political, military, social, and economic overlay can further note the penetration of these capabilities into regions of political turmoil and highlight how they may be networked to create nuclear weapons potential. We can correlate these with visible terrorist activities by groups with motivations, statements, and attacks that suggest an interest in weapons of mass destruction (WMD). These indicators can help in assessing risk and setting priorities, but these strategic indicators may become fewer and less clear in the future as latent WMD potential becomes even more widespread. Moreover, we have very little certainty of tactical warning and may get few precise actionable indicators of any WMD attack.

Because fissile material is essential to the nuclear devices terrorists may wish to acquire, it will come as no surprise that controlling and securing fissile material must be the highest priority, second only to protecting weapons themselves. At the same time, we must be careful not to recreate the mistakes of the Maginot Line. We can gain great leverage from sound physical security, especially when "guns, guards, and gates" are augmented by an effective system of material protection, control, and accountability. In the end, however, any linear defense will have vulnerabilities, particularly if an "insider threat" is involved. This is true in securing fissile material, and it is true in preventing the exploitation of dual-use technology. Worse, terrorist groups, as with other criminals such as drug cartels, money launderers, and smugglers, are becoming more adept at exploiting legitimate industries, activities, and individuals who unknowingly become a part of the network. In between the legitimate and black markets are not very well understood, but unsavory "gray" markets. Here too it is individuals with whom we seldom have contact who are more likely than we are to see activity related to illicit nuclear weapons related activity.

Thus, in the transition countries and other countries where we have concerns about security, we can help. The indigenous governments and institutions, however, must step up to the seriousness of the matter, take responsibility, and hold people accountable for adopting best practices and then testing their security measures and personnel to make them even more effective. Here too we can help even if they, not we, are more likely to have the right people at the right time at the right place positioned to do the right thing. They, like we, must have a dynamic strategy that takes into account that terrorists will probe and adjust until they determine a way ahead.

Essential to the success of the terrorists is the assistance of knowledgeable individuals – knowledgeable in the sense that they are good enough to solve the problems the terrorists face. In the case of nuclear terrorism, those problems may be how to overcome security at nuclear storage areas or how to work with radioactive material or how to design an explosive device. Terrorists are unlikely to begin at the basic research level, and they are unlikely to seek or find Nobel Prize winners to lead their programs, although totalitarian regimes have had access to numerous world-class talents. Terrorists are more likely to try to bring together journeyman skills related to proven paths, and they may be able to attract competent, if disgruntled or disturbed, people. The less they have to break new ground, the better from their perspective.

This is not to say they will follow exactly current or historic paths taken by nuclear weapons states. They may surprise us in their creativity. But they will need help and much of that help can only come from technologically savvy people, be they scientists, engineers, technicians, or just employees who know where things are located or how they work. The technology sector of American industry will tell you that the best form of knowledge or technology transfer is the transfer of knowledgeable people. There is no reason to believe it is much different in the case of terrorism.

The fact that terrorists need access to knowledgeable people gives us a further arena in which to counter the terrorists. Unfortunately, it cannot be said that all individuals in the technology sector would refuse to help terrorists. The history of crime and terrorism, unfortunately, includes a number of technical people including medical doctors who have taken professional oaths to protect lives. Ideological or theological extremists are to be found in the technical communities, which, however cosmopolitan, generally contain most elements of the views of the societies with which they most closely interact. Still, the technology sector is one populated predominantly by individuals who must interact with a wide range of people who do not share the goals, or at least the means of terrorists.

Much of the community of technologically savvy individuals is sensitive to the security concerns we have about terrorist access to dual-use technology or material, be it nuclear, chemical, biological, or other. Some are very aware of the dangers. Most operate in an environment that stresses security of intellectual property and industrial know-how. Many work in an export control environment. Important segments work on safety and security. Others work in areas such as sensors or vaccines that may provide countermeasures. The United States and its allies have considerable interaction with this community in the advanced economic sectors. We are less well connected to the scientific and industrial networks that operate in less advanced economies, especially within authoritarian regimes and troubled regions. Even here, however, there are contacts and means of influence. Engagement of these communities and industries through their

governments and directly is of great importance. In particular, we need to become more involved in the Islamic world.

I want to stress this need for broader engagement, layered defenses, and a dynamic strategy, in part, because the problem of the latency of potential destructive capabilities in developed and developing economies is bigger than the nuclear question. There is an unclear and present danger that governments, rogue officials, or non-state groups and individuals can exploit ever more widespread dual-use technology to obtain weapons of mass destruction or in other ways threaten great damage. I say unclear danger because so many capabilities can be networked in so many ways that it is difficult anticipate the precise use to which they will be put. I say present danger because the risks are here and now and include more than the nuclear. Indeed, many analysts believe that the greatest threat is biological.

Nuclear and biological attack clearly pose the most disastrous consequences. Still, we may also be under estimating the lesser dangers that are associated with chemical attacks and conventional attacks. The modern global economy is highly leveraged. We must not let the complexity of economic activity and our spirited efforts at recovery after the September 11, 2001, attacks lead us to underestimate the total economic cost of both the cumulative harm over time and the steps taken in response. We are fortunate that we were able to manage our way through this period without greater economic disruption. We cannot rule out, however, the possibility that a series of major terrorist attacks, especially if involving WMD and especially nuclear weapons, could push the world into an economic depression with devastating political and social consequences that are not lost on the terrorists who might want to bring this about.

Modern societies will have to do a better job of understanding the latent capacities for destructiveness in our societies. We need a better assessment of our vulnerabilities, and we need to do a better job of managing the risks. By "latent" capacities, I mean what the dictionary defines as "potentially existing, but not presently evidence or realized." We need to understand the degree to which the potential to acquire, deploy, and use WMD is becoming more accessible to more players (state, quasi-state, and non state) for more deadly goals against our citizens and interconnected societies. We need to build a dynamic strategy that recognizes that our reaction times will be short because the lead times for terrorists may become much shorter and our ability to observe their preparations weaker. This will put a premium on prevention. It will put a premium on active strategies for intelligence and law enforcement.

When you are looking for a needle in a haystack, it helps to have a tool like a magnet. "Sting operations" play an important role despite their limitations. Recognizing that terrorists are attracted to vulnerabilities and icons may improve our chances of detection. Similarly, choke points and boundaries can increase the chances of detection. Going to the source by infiltrating or monitoring terrorists groups and those they seek to exploit to obtain weapons capability becomes more important. Most of these activities involve intelligence and law enforcement and must be undertaken by governments. The governments that may prove to be best positioned to deal with terrorists may be governments elsewhere. Terrorism is a multinational problem, and

multinational solutions, such as closer cooperation among intelligence and law enforcements agencies, especially in combating nuclear materials trafficking, are needed to deal with it.

Many governments are stepping up to the terrorist problem, but many are not engaging effectively on the WMD challenge as it relates to terrorism any more effectively than they have dealt with the problem of the spread of nuclear weapons to nation-states. The reasons are clear. Governments themselves have competing goals and interests. Many enabling technologies are too widespread to monitor cheaply and effectively. Modern business networks with "just in time" inventories, offshore outsourcing, flat-almost virtual organizational pyramids, numerous competitors, and multi-tiered markets are amorphous and changing. Universal norms seem inappropriate in specific cases. Enforcement options are unattractive.

We run the risk of replaying the old debate over whether the technologies are the problem or those that use them are the problem. We won't be effective until we recognize that action must be taken on both fronts. We need only look at the problem of nuclear proliferation among nations to see that we are in danger of making the same mistake with respect to terrorism, i.e., assuming that if we put in place measures to control material, we have solved the problem. These safeguard measures have helped, and helped greatly. But for too many years, the international community relied too heavily on IAEA safeguards of declared material and declared facilities while it sought to avoid addressing the more complex issues of motivations, planned latency, covert programs including non-materials related activity, third-party assistance, non-state actors, and treaty break-out. Even now that these risks have been so clear, we do not have in place the means to deal effectively with clear violations of the NPT.

Again, we run the risk of making the same mistake on the terrorist front. To treat fissile material as if it were the gold in Fort Knox has the right spirit. Unfortunately, the better analogy may be to armored cars, bank vaults, or art masterpieces in museums. Every now and then there is a heist, carefully prepared– sometimes with the help of an insider. Since we must deal with conventional, biological, and chemical terrorist threats in which we cannot rely so heavily on materials controls, we should look toward a synergistic strategy for dealing with nuclear terrorism that is also proactive.

Deeper cooperation among nation-states in intelligence and law enforcement can be supplemented by counter-WMD cooperation such as in the Proliferation Security Initiative and by the fulfillment of the potential of UNSC 1540, which moves to hold governments accountable for measures to prevent non-state actors from acquiring WMD. Across the board, we need to roll up our sleeves and work together more at the detailed level. In this context, more extensive and advanced cooperative threat reduction that involves embedded engagement with scientific, technical and industrial communities around the world will be necessary to improve understanding of the problem and develop countermeasures. It may also give us more hope that there will be someone at the right place at the right time who does the right thing.

Thank you.