Testimony before the
Subcommittee on Technology and Innovation
Committee on Science and Technology
United States House of Representatives

"BIODEFENSE IN THE DEPARTMENT OF HOMELAND SECURITY FY08 SCIENCE AND TECHNOLOGY BUDGET"

March 8, 2007

A Statement by

GERALD L. EPSTEIN

Senior Fellow for Science and Security
Homeland Security Program

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, 1800 K STREET, NW, WASHINGTON, DC 20006
TELEPHONE: (202) 887-0200; FACSIMILE: (202) 775-3199 WWW.CSIS.ORG

Testimony of Dr. Gerald L. Epstein
Senior Fellow for Science and Security
Homeland Security Program
Center for Strategic and International Studies
Washington, DC

Subcommittee on Technology and Innovation
Committee on Science and Technology
U.S. House of Representatives

"Biodefense in the Department of Homeland Security
FY08 Science and Technology Budget"

March 8, 2007

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to appear before you today to discuss the Department of Homeland Security's Science and Technology Budget for Fiscal Year 2008. I am currently serving as Senior Fellow in Science and Security in the Homeland Security Program at the Center for Strategic and International Studies (CSIS), here in Washington. I am also an adjunct professor at Georgetown University's Edmund A. Walsh School of Foreign Service, where I teach a course on science, technology and homeland security. I have been working in the area of science, technology, and security policy for more than twenty years and have been studying nuclear, chemical, biological, and radiological weapons issues and responses for over 15 years.[1]

At CSIS, my colleagues and I are involved in a major international effort, supported by the Carnegie Corporation of New York and the John D. and Catherine T. MacArthur Foundation, to take a comprehensive, international, and interdisciplinary approach to dissuading, interdicting, mitigating, and responding to biological weapons threats. This project aims to improve the ability to counter these weapons at all stages, from influencing the intent to produce weapons, to denying access to materials and expertise, to detecting illicit programs, to managing the consequences of an attack. The Department of Homeland Security's Science and Technology program, and particularly its biological defense programs, are an important part of the United States'—and the world's—response to these threats.[2]

Other Sources of Advice to Congress

Before I start, however, I cannot help pointing out to this Committee that I first started working on the issues I will be discussing today at an agency that no longer exists—the Congressional Office of Technology Assessment. At OTA I was the project director for a major series of reports produced for the Congress on the proliferation of weapons of mass destruction, including biological weapons. As much as I welcome the opportunity to discuss these issues with members of this Committee this morning, frankly you and your colleagues deserve more attention than I or any other outside witnesses can devote to you in one hearing. You need a dedicated, credible, and authoritative body of substantive experts, working for you within a carefully structured and fully bipartisan process, that can relate the best available technical

understanding directly to the policy choices you face. I have long believed that you and your colleagues—who must act on policy issues that are inextricably dependent on science and technology in practically every Committee of Congress—would find such a capability to be very helpful.

Homeland Security Science and Technology Challenges

What we now call "homeland security" has only been recognized as a mission of the federal government since the late 1990s, and only since 9/11 has it acquired the resources and organization it has today. Previously, national security policy dealt primarily with overseas threats, and domestic policy did not have a major security component. The U.S. National Academy of Sciences' landmark 2002 study *Making the Nation Safer*[3] recognized the vital role that science and technology could play in bolstering our homeland security, and this report played a significant role in the establishment of a Directorate of Science and Technology within the new Department of Homeland Security (DHS) in 2003. Given both the importance of applying science and technology to this new mission and the paucity of previous government efforts to do so, the DHS S&T Directorate was one of the few parts of the new Department to receive a substantial infusion of new funding; most of the rest of the Department consisted of agencies whose staffs, budgets, and missions were transferred (either whole or in part) from elsewhere in government.

The Department of Homeland Security's Fiscal Year 2008 budget request marks only the fourth one that has been prepared by the Department itself, as opposed to its various predecessor agencies, and applying science and technology to the homeland security mission continues to pose challenges:

1. ***Military technology is not directly applicable to homeland security.*** Although the military has considerable experience in developing and fielding technologies that are relevant to homeland security needs (such as detecting chemical and biological agents), few military systems can be directly adopted in a homeland security context. Military and civil users differ in their threat scenarios; levels of user skill, experience, and training; systems for maintenance, logistics, and self-protection; sources of funding; willingness to tolerate disruption; ability to issue orders; and respective legal and policy contexts in ways that make it very difficult to use military systems for homeland security purposes. The independent existence of a DHS Science and Technology program is an acknowledgment of this fact.

2. ***Users of homeland security technologies may not be federal employees.*** Many individuals responsible for mitigating, defending against, or dealing with terrorist attacks in the United States—e.g., police officers, emergency medical technicians, subway train operators, operators of critical infrastructures—are not federal employees at all. They work for state, local, and tribal governments or for the private sector, often in organizations that buy equipment "off the shelf" and that have little experience in developing their own systems. They may even be members of the public attempting to protect themselves. These users tend to be highly disaggregated, and they may not have their own funding to purchase and field new technologies.

3. ***Users may not even exist yet.*** Some key missions of interest to the DHS S&T directorate—including detection of pathogenic biological organisms in the atmosphere, decontamination of wide areas after a major biological attack, or detection of smuggled nuclear weapons in commercial shipping—were nobody's responsibility prior to the creation of DHS. Moreover, technological breakthroughs can provide capabilities that had never been anticipated, and that no institution or entity may currently be in a position to utilize. Although developing technology without a clear sense of what is needed risks wasting time and money, tying R&D programs exclusively to the identified needs of established users can impede our ability to utilize "game-changing" breakthroughs. Sufficiently powerful tools should motivate us to figure out how to use them.

4. ***Technologies don't protect us—systems do.*** Throwing technology at a problem does not necessarily make us safer. Careful studies are needed to identify systems and concepts of operations that will mitigate, dissuade, expose, or respond to threats; model how effectively these systems will work in different situations; ask how the deployment of such systems might change the nature of the threat; and evaluate how much better off such a system, on balance, will make us. Moreover, the political leaders who will oversee the use of these systems need to become familiar with their capabilities and their limitations.

5. ***Prioritization is, and will remain, difficult.*** Perhaps the hardest job in developing homeland security technologies is determining which threats to address, deciding how much to spend on countering each, and measuring our progress. Major terrorist attacks are fortunately rare, and we do not have an exhaustive database of prior attacks that will let us predict what the next attacks will look like. Moreover, tracking terrorist plans and capabilities is much more difficult, say, than counting Soviet armored divisions or intercontinental ballistic missiles was. Modeling and systems studies can provide some guidance in allocating our defensive dollars, but they can be very sensitive to assumptions that will be impossible to justify empirically. Improving our methodologies for such decisionmaking should itself be a high priority, even if in the end, decisionmakers will have to rely on subjective judgment.

6. ***No magic organizational solution can eliminate inherent overlap among agency missions,*** such as those of the Department of Homeland Security and the Department of Health and Human Services (HHS). DHS deals with deliberate attacks, including those involving biological agents and disease. HHS deals with health and disease threats, including those involving deliberate attack. Biological attacks are both health incidents and security incidents, and both DHS and HHS must be involved in countering them. The potential for conflict can never be eliminated, but it can be managed—particularly through open lines of communication, clear delineation of roles and missions, and an awareness of the different contexts in which each agency views this issue.

Biodefense in the FY 2008 DHS Science and Technology Budget

The largest component of the DHS S&T Directorate's budget is the Chemical and Biological Division, which I was asked to address in my testimony. Overall federal responsibilities for biodefense and biosecurity have been specified in policy documents such as Homeland Security Presidential Directives HSPD-9 ("Defense of United States Agriculture and Food,"), HSPD-10 ("Biodefense for the Twenty-First Century"), and HSPD-18 ("Medical Countermeasures against Weapons of Mass Destruction"), which in turn have generated taskings for the Department of Homeland Security. A few aspects of the Department's biological research and technology development program merit particular attention.

Prioritization. As indicated above, one of the key management challenges facing those responsible for developing and deploying homeland security technologies is establishing priorities. At the operational level, this process would consist of identifying performance or readiness goals that characterize the capabilities we need to achieve; measuring how far we are from those goals; and deriving a set of programs (including acquisition, technology development, training and doctrine, etc.) that will close those gaps. This process would also require some way of evaluating which gaps were most important to close, and which programs would be most effective in closing them. Such a process would involve all agencies that had homeland security responsibilities, and it would be updated regularly.

The National Academies' study *Making the Nation Safer* stated that the government did not have the analytic capabilities it needed to inform decision making,[4] and it called for such capabilities to be created. That work is incomplete. Even with better tools, however, I believe that assessing risk, setting priorities, and measuring progress will be a very difficult job—one that is harder than the equivalent planning process in the Department of Defense, since homeland security vulnerabilities are more diverse and the threats against them harder to evaluate. In the end, however, dollars have to be spent on some things and not on others, and those choices should be informed by analysis to the greatest extent possible.

Biowatch and the Office of Health Affairs. The transfer of operational responsibility for the Biowatch system into the new Office of Health Affairs for FY 2008 budget is a promising development.

The Biowatch system, which samples air in a number of metropolitan areas for the presence of specific biological threat agents, is an example of a system that was deployed before it had true users. We had never had the ability to respond to a bioterrorist attack on a U.S. city in "near real time"—as or shortly after the agents were released—and it was therefore nobody's job to look for attacks on that timescale. Nevertheless, the motivation for the Biowatch system is compelling—to provide sufficient warning to initiate the distribution of medical countermeasures before illnesses start to manifest, when those countermeasures can be far more effective.

The combination of a compelling technical rationale with the lack of an obvious user meant that the early deployment of this system outpaced the development of response protocols that involved all the local, state, federal, and nongovernmental entities that would have some role in responding to a true attack. In subsequent years, as we have gained experience operating this system, additional work has been done to incorporate Biowatch information more effectively

into response planning and decisionmaking. Even so, it remains an open question whether or not Biowatch will be able to provide early confirmation of a biological attack with a level of confidence that is high enough for public officials to take highly consequential actions such as community-wide distribution of medication.

Exploration of these essential systems issues will be advanced by the transfer of operational responsibility for running the Biowatch system from the DHS Science and Technology Directorate to the new DHS Office of Health Affairs. The S&T Directorate would retain responsibility for technical improvement and next-generation systems. This transfer for the first time identifies a principal federal "user" for the Biowatch system, albeit a surrogate one. The Office of Health Affairs does not itself mount the full response to a biological attack, but it does have the responsibility to work with actual responding agencies at many different levels of government to ensure that the Biowatch capability is effectively utilized. Clarifying operational and research responsibilities for the Biowatch system is a positive step that will improve both the technical prospects and the operational confidence of the system.

Technically, Biowatch has been highly successful. I would never have predicted that over two million Biowatch assays would have been processed by now without any false alarms. This is a very impressive record that helps to build confidence in the system. At the same time, we have seen a number of "true positives"– the detection of actual threat agents in city air samples. In each case, these detections have been attributed to organisms that occurred naturally in the environment, and none of these detections resulted in mobilizing a full response to a fictitious attack. These detections therefore served to validate the system hardware and analysis protocols, and they also proved that our response protocols did not incorrectly assume a detection always meant an attack.

On the other hand, the fact that Biowatch alarms had to be confirmed by actual cases of disease before a full response would have been mounted does raise the question of what the added value of the Biowatch system is. (Note that the response to an alarm might have been different for an agent such as smallpox, which is not found in nature, for which confirmed laboratory detection would be impossible to attribute to natural causes.) As we continue to gain operational experience with Biowatch, it will be essential for the Office of Health Affairs to evaluate the ways in which Biowatch warning information can prove useful, even if it is not sufficient to trigger a full response. Possible uses of such information include heightening our sensitivity to look for individual cases of disease, triggering some initial stages of pharmaceutical distribution, or informing subsequent determination of the scale and scope of a biological attack.

Relationships Between DHS and Other Governmental Agencies. As described above, there is no organizational solution that will eliminate the potential for interagency conflict or confusion over biodefense. As we are exploring at CSIS in our Biological Threat Reduction project, interactions between different professional communities—embodied in the U.S. government by different government agencies—are an essential aspect of any response to biological threats. Although these interactions will always present challenges, I believe that the Departments of Homeland Security and Health and Human Services are developing appropriate mechanisms for working together.

In the current fiscal year—pending appropriations—and certainly in the coming year, a new agency in the Department of Health and Human Services will appear on the scene with a vitally important role in biodefense: the Biomedical Advanced Research and Development Authority, or BARDA. With the mission of bridging the gap between basic biomedical research and countermeasure procurement, BARDA will play an essential role in building the nation's capacity to respond to biological attack. But in addition to facilitating the development of specific countermeasures, BARDA will have an additional mission that may prove even more important in the long run—that of promoting innovative technologies that can reduce the time and cost of countermeasure development in general. With biotechnology becoming ever more powerful and more widely available, we will be less and less able to restrict our attention in the future to a short list of threat agents, each with its own lengthy and expensive countermeasure program.

Instead, we have to move towards a flexible, adaptive, and responsive biodefense system capable of dealing with threats in near-real-time. Creating such a system will blur the distinctions between environmental detection, medical diagnosis, prophylaxis, and treatment, making it even more important for the Departments of Homeland Security and Health and Human Services—whose mission delineations currently depend on some of these functional boundaries—to work together effectively. These departments will also need to work with the Department of Defense, whose Transformational Medical Technologies Initiative, funded by the Defense Threat Reduction Agency, also works to shorten and simplify medical countermeasure development.

Time and Risk Horizon of DHS Research. When the Department of Homeland Security's Science and Technology Directorate was first formed, there were so many immediate demands for science and technology that longer-term research was considered an unaffordable luxury. This may have been a necessary decision at the time, but it was not a sustainable one. Failure to invest in longer-term research limits the prospects for future breakthroughs that could dramatically improve DHS's ability to fulfill its mission.

As the S&T Directorate matures, so must its S&T portfolio—which means investing in a portfolio of both near-term and long-term research. I understand that the S&T Directorate's leadership now shares this view. I particularly welcome Admiral Cohen's plans to fund some high-risk but potentially very high payoff projects. A serious pathology that can overtake a technology development program is to become failure intolerant, forcing it to settle on safe bets that are less ambitious than its mission requires. Admiral Cohen will need your support if he hopes to avoid this—you will have to make sure he fails often enough, and to hold him accountable if he doesn't.

Classified Biological Research and Treaty Compliance. Classified research constitutes a much smaller portion of the U.S. biodefense program than many might suspect. The vast majority of U.S. biodefense consists of unclassified research at the National Institutes of Health, which dwarfs *all* Department of Homeland Security biodefense activities, let alone any classified ones. Nevertheless, classified DHS biodefense research will constitute one of the most controversial parts of the U.S. biodefense program. Research that cannot be shared with diverse technical reviewers, independent non-Governmental observers, or foreign colleagues will raise questions with respect to technical merit, policy appropriateness, and treaty compliance.

Even more so than in other areas of science, the biological sciences have enjoyed a tradition of openness and international collaboration—and this heavy presumption of openness should continue. Since disease continues to kill millions of people around the world each year, any restrictions on relevant scientific knowledge could have serious consequences. Yet the existence of hostile, witting adversaries that are determined to wreak devastation and that are known to be interested in biological weapons mandates that this openness not be absolute. The U.S. biodefense program would like to avoid serving as the R&D program or the targeting staff for Al Qaeda or any other terrorist group, even while it works to advance science, cure disease, and assure the world that it is abiding by treaty commitments.[5]

Without attempting to do justice to the complexity of this issue, let me make a few observations about both classification and treaty compliance:

- Actions that violate the 1975 Biological Weapons Convention (BWC) also violate similarly worded provisions of U.S. law.[6] Any government employees or contractors who violated the BWC in the course of their job would be subject to criminal prosecution.
- DHS should engage in public outreach to instill confidence that it is appropriately reviewing its biological research activities, including classified activities, for treaty compliance, legal compliance, and consistency with policy.
- No matter how rigorous its internal review policies are, and notwithstanding the involvement of officials who have no connection to the projects being reviewed, an internal DHS compliance process will not be viewed by outside observers as being truly independent. The more widely that DHS activities, including classified ones, can be reviewed by appropriately cleared individuals outside of DHS and even outside the U.S. government, the greater the confidence will be that the Department's activities are technically sound and treaty compliant.
- Even if it cannot all be shared with the public, the United States has an interest in sharing information on its biodefense activities with other countries to assure them that it is complying with the Biological Weapons Convention. The fact that the United States has no offensive biological weapons program should allow it to share this information more widely than if it were seeking to protect a military advantage.
- Classified biodefense activities have been accused of triggering a "security dilemma"—of appearing to others as offensive, and therefore stimulating other countries to respond with offensive programs of their own.[7] Independent of the level of empirical support for this proposition—there are certainly examples of state biological weapons programs that proceeded in, or were even prompted by, the *absence* of any perceived bioweapons activities by their adversaries[8]—this argument retains at least theoretical salience as an incentive for openness. However, it is incomplete at best. It is not clear that a country suspecting others of having offensive biological weapons programs would choose to respond with an offensive program of its own; a much more rational response would be for it to improve its defenses. Even more significantly, the argument fails utterly with respect to non-state programs. Al Qaeda's motivation for pursuing biological weapons,

for example, has absolutely nothing to do with any suspicion that the United States may have an offensive program.

- The Biological Weapons Convention bans the development of biological agents "of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes."[9] The treaty has no meaning if any conceivable offensive activity is justified as "protective" on the grounds that it is important for defensive purposes to "see what is possible." Although some may worry that classified U.S biodefense efforts may be doing just that, I believe that the U.S. biodefense program has too much to do to waste resources on such unconstrained speculation, even without treaty restrictions. However, I also believe that a requirement to be protective can be made operational in a treaty compliance review. To justify an activity as "protective," I would argue that it should be shown to specifically increase our ability to protect ourselves—e.g., that its results should directly and materially inform particular decisions, or contribute to particular capabilities, that improve our ability to protect against biological weapons.

Human Resources for Homeland Security Related Science and Technology. One farsighted program run by the DHS Science and Technology Directorate is its Graduate Fellowship program. This program is intended to support outstanding graduate students in technical disciplines that are important to the DHS mission, with the ultimate objective of strengthening the nation's science and technology community. However, more can be done to attract these Fellows into careers in the homeland security sector.

Fellows are required to attend an orientation program, to participate in a 10-week internship, and to express willingness to accept homeland security-related employment after graduation (although this is not a binding obligation). U.S. citizenship is required, and security clearances are required for many of the internships.

A strengthened S&T community constitutes "a critical advantage in the development and implementation of counter-terrorist measures and other DHS objectives," as the Fellowship's promotional materials explain,[10] but having these Fellows enter the technical community at large upon graduation does not serve the homeland security mission as effectively as if they were to work directly in the homeland security sector. The United States scientific and technical workforce is strongly dependent on foreign nationals, who constitute a significant fraction of each year's graduates in technical disciplines. Many of these highly skilled foreign nationals remain in the United States after graduation, to this country's great benefit.[11] However, foreign nationals are not eligible to work in many homeland security-related institutions. DHS Graduate Fellows can, and policies that maximize the fraction of these technically trained U.S. citizens who enter the homeland security sector would be very valuable.

The current program exposes Fellows to DHS problems and processes to some degree, but I think that a deeper level of engagement with these Fellows, with a more thorough exposure to the U.S. government's homeland security operations, will stimulate greater interest in pursuing homeland security careers after graduation. More should be done to secure security clearances for the Fellows and brief them on homeland security threats at a classified level; to have senior representatives from homeland security and related agencies (i.e., homeland security, intelligence, defense, public health, critical infrastructure) meet with them to describe their jobs,

their agencies' responsibilities, and different ways in which science and technology build homeland security capabilities; and to establish mentorships between Fellows and senior employees in the homeland security sector. The Fellows should be convened periodically, perhaps by holding regional meetings or seminars that would be convenient for them to attend. Ongoing engagement with the Fellows is much more likely to elicit an interest in a career in homeland security than a single orientation.

A model for such a program of continuous engagement and involvement of technical professionals in security problems, albeit one pitched at a smaller number of individuals at a more senior level in their career, would be the Defense Science Study Group that is organized by the Institute for Defense Analyses for DARPA. I would recommend that DHS officials involved in the Graduate Fellowship Program familiarize themselves with that activity.

Mr. Chairman and members of the subcommittee, I thank you for your interest, and I would be pleased to answer any questions you may have at this time.

NOTES

[1] None of the institutions I am affiliated with take policy positions on the topics I will discuss, and the views expressed are strictly my own.

[2] See the CSIS Biological Threat Reduction Program website at www.csis.org/hs/btr

[3] Committee on Science and Technology for Countering Terrorism, National Research Council; *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism* (Washington, DC: National Academy Press, 2002). Available online at http://www.nap.edu/html/stct/index.html

[4] *Ibid*, p. 21.

[5] See Center for Strategic and International Studies, Commission on Scientific Communication and National Security, *Security Controls on Scientific Information and the Conduct of Scientific Research* (June 2005) for discussion of some of the tensions between security and openness. This paper is available at http://www.csis.org/media/csis/pubs/0506_cscans.pdf [underscore between "0506" and "cscans"]

[6] Biological Weapons Anti-Terrorism Act of 1989, now at Title 18, Section 175 of the United States Code.

[7] Jonathan Tucker, "Avoiding the Biological Security Dilemma: A Response to Petro and Carus," *Biosecurity And Bioterrorism: Biodefense Strategy, Practice, And Science*, Vol. 4, No. 2 (2006), pp. 196-197

[8] W. Seth Carus and James B. Petro, "Avoiding the Biological Security Dilemma at Our Own Peril: A Response to Tucker," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, Vol. 4, No. 2 (2006), p. 202.

[9] Biological and Toxin Weapons Convention, Article I(1)

[10] "DHS Scholarship and Fellowship Program 2007 Competition Guidelines," http://www.orau.gov/dhsed/

[11] See Center for Strategic and International Studies, Commission on Scientific Communication and National Security, *Security Controls on the Access of Foreign Scientists and Engineers to the United States* (October 2005) for discussion of the importance of foreign interchange to the U.S. science and technology base. This paper is available at http://www.csis.org/media/csis/pubs/051005_whitepaper.pdf [underscore between "051005" and "whitepaper"]