SCIENCE AND TECHNOLOGY FOR HOMELAND SECURITY

Statement of
Lewis M. Branscomb
Emeritus Professor of Public Policy and Corporate Management; and Emeritus Director of the Science, Technology, and Public Policy Program, Center for Science and International Affairs
John F. Kennedy School of Government, Harvard University, Cambridge, Mass.
and
Co-chair, Committee on Science and Technology for Countering Terrorism
National Research Council
The National Academies

before the
Governmental Affairs Committee
U.S. Senate

JUNE 28, 2002

Good morning, Mr. Chairmen and members of the Committee. I am Dr. Lewis M. Branscomb, Emeritus Professor of Public Policy and Corporate Management; and Emeritus Director of the Science, Technology, and Public Policy Program in the Center for Science and International Affairs at the John F. Kennedy School of Government of Harvard University. I also served as co-chair of the Committee on Science and Technology for Countering Terrorism of the National Academies' National Research Council. I am here today to discuss the contents of this committee's report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, and also to offer my views as an individual on issues related to effective use of science and technology by the proposed new Department of Homeland Security.

National Academies Report on Science and Technology for Countering Terrorism

Let me thank the committee for the opportunity to describe the National Academies' Report on science and technology strategies for responding to the threat of catastrophic terrorism (hereafter called the Report).[1] While our report was completed before the President's Bill to create a Department of Homeland Security (DHS) and thus does not contain an analysis of this proposal, the committee did have the chance, following the President's June 6, 2002 speech, to consider the possibility of such a department. The Report makes two important recommendations in that area. In any case, we believe that useful guidance on how effective any proposed organization for the new department might be could be gained from looking at whether that organization allowed the government to carry out the recommendations made throughout the Report.

The report identifies key actions that can be undertaken now, based on knowledge and technologies in hand, and, equally importantly describes key opportunities for reducing current and future risks even further through longer-term research and development activities. However, science and technology are but one element in a broad array of potential approaches to reducing the threat of terrorism. Diplomacy, international relations, military actions, intelligence gathering, and other instruments of national policy well beyond the scope of this study all have critical roles to play.

Our society is too complex and interconnected to defend against all possible threats. As some threats are diminished others may arise; terrorists may change their goals and tactics. While this report describes what in the committee's best judgment are the top-priority actions and research objectives for harnessing science and technology to meet today's threats, the most important conclusion of this report is that the nation needs a well-organized and disciplined ability to respond as circumstances change. In that sense this is not an enduring plan for technical work, but rather a starting point from which the nation can create defenses-in-depth against the new threat. For that reason it is especially important that strengthening the national effort in long-term research that can create new solutions be a cornerstone of the strategy for countering terrorism.

The Report provides a technical roadmap to guide the initial response to the threat of catastrophic terrorism. It is not a plan. Our primary concern is the competence of the governmental units to undertake the tasks they now confront. The main body of the report contains a very large number of technical recommendations (some 134 of them). The committee felt strongly, however, that give the unusual nature of the threats the terrorists pose and the fact that the federal government is structured for Cold War, and not for this new threat, that we must confront the question of how our technical recommendations could most effectively be put to good effect.

Research performed but not exploited, and technologies invented but not manufactured and deployed, do not help the nation protect itself from the threat of catastrophic terrorism. In this report, the committee urgently recommends a number of steps to ensure that technical opportunities are properly realized. In particular, in recognition of the importance and difficulty of determining goals and priorities, the committee discusses how the federal government might gain access to crucial analytic capabilities to inform decision making—allowing improved assessment of risk and of the effectiveness of measures to counter risk.

Most important is that there be a federal office or agency with central responsibility for homeland security strategy and coordination and that this organization have the structure and framework necessary to bring responsibility, accountability, and resources together to effectively utilize the nation's science and engineering capabilities. The committee believes that the technical capabilities to provide the analysis necessary to support this organization do not currently exist in the government in a unified and comprehensive form. Thus the committee recommends the creation of a Homeland Security Institute to serve the organization setting priorities for homeland security.

This institute would provide systems analysis, risk analysis, and simulation and modeling to determine vulnerabilities and the effectiveness of the systems deployed to reduce them; perform sophisticated economic and policy analysis; manage red-teaming activities; facilitate the development of common standards and protocols; provide assistance to agencies in establishing testbeds; design and use metrics to evaluate the effectiveness of homeland security programs; and design and support the conduct of exercises and simulations. The committee believes that to function most efficiently, this institute should be located in a dedicated, not-for-profit, contractor-operated organization.

In the current structure, the primary customer for this Homeland Security Institute would be the Office of Homeland Security, which is currently responsible for producing a national homeland security strategy. Whether this office will also be responsible for monitoring progress on this strategy and revising it in the future is not clear. On June 6, 2002, the President proposed a reorganization in which many of the agencies and programs operating on the front line of counterterrorism would be brought together to form a new Department of Homeland Security. However, even within this department, the programs with the expertise and experience in science and engineering research would not necessarily be closely connected to the units with the responsibility for technology deployment. Perhaps more important, the federal agencies with the best access to the nation's sources of scientific, engineering, and medical research capability lie outside the proposed department, and close connections with these groups will be needed to allow the department to produce the best-quality effort on counterterrorism.

Thus, however the leadership of the federal effort in homeland security is organized, the government will need mechanisms to engage the technical capabilities of the government and the nation's scientific, engineering, and medical communities in pursuit of homeland security goals. Today the focus is on determining these goals, and the link between the Office of Homeland Security and the Office of Science and Technology Policy is a key element in setting the science and technology component of the national counterterrorism strategy. This link will continue to be essential, but if a new department is formed it will not be enough. A new department will need an Undersecretary for Technology to provide a focal point for guiding key research and technology development programs within the department and connecting with relevant technology agencies outside it. In addition, the Office of Homeland Security will need to work closely with the Office of Science and Technology Policy, perhaps through the National Science and Technology Council, on coordinating multiagency projects and their linkages to related programs devoted primarily to other high-priority national objectives.

Effective use of science and technology by the proposed new department

Let me now provide you my own views, which the committee requested. These views go beyond the work of the Academies, which, as noted above, did not have the opportunity or the assignment to evaluate alternative structures for a Department of Homeland Security. Thus, I am pleased to respond to your request to me, speaking as an individual and not for the Academies or its committee on counterterrorism, to give you my personal views about the structure of the President's proposal. I am happy to do so, with that understanding – that I speak for myself, with my views largely colored by over 20 years of service in the federal government, 14 years as chief technical officer and member of the management committee of IBM corporation, and 16 years as a professor of S&T policy at Harvard University.

Perhaps the most useful thing to do would be to discuss the strengths and weaknesses of the President's Bill as submitted in relation to the mobilization of the nation's technical talents and assets in the cause of homeland security.

Strengths and weaknesses of the President's bill

A casual reading of the missions of the four operating units of the proposed department (Titles II – V) clearly shows DHS to be a highly technical organization. The Department is to be comprised of the agencies and units that have important operating responsibilities required for combating terrorism. I believe the list of component parts, taken together with the mission and authority of the Department, covers most of the identified threat types and areas of vulnerability, although not with equal emphasis. Because the terrorist threats are unlike those of conventional war, and their targets are elements of the civil population and infrastructure, the response by the Department must be not only technically sophisticated but also highly creative and flexible.

The divisions created by Titles II through V are structured so that the agencies and units of which they are comprised can continue with as little disruption as possible, except for the primacy of homeland security as the new priority for their activities. Also the bill has a commendable provision to allow creative human resource policies. I also commend the provision allowing the President to restructure the Department internally, once experience suggests changes to make it work better.

I have three primary suggestions about the *structure* as it stands in the President's Bill:

- Operating and support functions are mixed and the missions of the Divisions established by Titles II – V are highly interdependent.
- It is very important that the Department have a senior technical officer at the rank of undersecretary for the whole department, with responsible for the Department's R&D budget.
- An R&D function that serves all the responsibilities of the department is needed.

Mix of operational and support functions in each of the divisions.

There is probably no way to avoid the fact that many if not most of the threats our study identified will require collaborative effort by all four divisions. That is certainly better than two dozen agencies with no central management as we have now. The first problem I see is that each of the four operating units has both divisional operational missions and support functions for all the other divisions. This split responsibility is likely to cause a loss of focus and to make the balance of internal and external responsibilities hard to manage.

The Title II division has not only an operating mission in intelligence and infrastructure protection, but also has what I see as vital staff support functions required for making the strategy in support of all the divisions: tasks (2), (3) and (4) in section 201 of Title II. Task (5) is an operating mission: "taking…necessary measures to protect the key resources and critical infrastructure…" If, in this phase, "critical infrastructure" means only information and communications infrastructure,[2] this should be made clear and the responsibility should stay in the Title II division. However, if "critical infrastructure" means *all* critical infrastructure (IT and physical), then perhaps this task should be assigned elsewhere, and this Title II division could become the analysis, planning and evaluation division of the Department.

The Title III division has vital operational roles in interception and countering of weapons of mass destruction

(WMD) – task (1) in section [301 Title III]. Task (3) specifically charges this division with establishing priorities for and conducting R&D and procurement of systems for protecting against weapons of mass destruction. Yet task (2) assigns to this division responsibility for R&D support of the entire for the whole mission of the Department. It is almost certain that the division's responsibility for both WMD operations and WMD research and development will cause it to give short shrift to R&D related to countering the array of threats that depend on weapons not considered WMD – e.g. explosives, industrial chemicals, food contaminations and agricultural attacks, and radiological or cyber attacks. Thus the two concerns about this division are (a) it has a mix of operational and support roles in this division, and (b) its duty to provide R&D in support of all the Department's needs will be in conflict with the R&D needs of the WMD mission.

The Title IV division has mostly an intercept mission, except for the broad charge to protect the transportation systems, and I assume to prevent them from being used as delivery systems for attacks. This is a very broad and difficult challenge, involving much more that threats from aviation. This capability depends on (a) what the division can get in the way of R&D support from the Title III division, (b) analytical support from the Title II division, and (c) the capability of TSA. TSA is to be a 60,000 person, multi-billion dollar agency, but no one that knows it well is optimistic about its ability to do the technical analysis, planning, R&D, acquisition and deployment of systems necessary to support of all the modes of transportation and protect their infrastructures. Giving TSA this capability will be one of the highest priority tasks of the new department. Substantial R&D funds will need to be allocated to TSA; it should not have to depend on the nuclear physicists and biologists in the Title III division.

The Title V division creates the plans for response and recovery, but this mission is separated from the threat analysis done under Title II. They need to be tightly linked. Also the response and recovery operations need to be supported by the same sensor networks and data mining capabilities required for detection and prevention of attacks.

In none of the task statements in Titles II, III, IV or V, do I see the assignment of responsibility for an array of important issues that lie outside information technology (Title II), WMD (Title III), Borders and Transportation (Title IV), and support for emergency services (Title V). These include standards for combined explosion and fire in buildings, filtering the air in high population buildings, developing biometric technologies, tagging explosives, protection of water supplies, etc...

Need for an integrated (over threats and over vulnerabilities) technical capability.

The most important conclusion of the Academies' study is that an integrated, systemic approach is needed to all of the threats and vulnerabilities, so that the threat analysis, the protection and recovery strategies and the final forensic measurements are consistent. Furthermore there are technologies that cut across all the threats. The report has a specific institutional recommendation for an non-profit, contractor-operated organization of systems analysts and technical domain specialists to assist the Department by providing threat analysis, modeling vulnerabilities, threats, and proposed protective systems, and generating tests of their effectiveness. These capabilities are needed to support decisions that the Secretary will have to make. In the report this is called the Homeland Security Institute.[3]

A chief technical officer at the rank of undersecretary for the whole department

The department must have a chief technical officer reporting to the Secretary. No high tech corporation tries to operate without this structure. The key choices involving technology investments are too important to leave to lower levels; they rise to the level of the Secretary. But the Secretary needs a senior executive (at the Undersecretary level) with the technical skill and legitimacy to support the secretary's decisions, to be the Department's key person in the government-wide technical councils such as the NSTC, and to build the relationships with the vital science and engineering agencies of the government: NSF, NIH, DOE, DOD, NASA, etc. Most important, it is to this executive that all the flows of technical analysis and strategy should come. She or he would also be responsible for the quality of all the R&D in the department and have the right of review and approval of top technical manager appointments. The Homeland Security Institute, described in the previous section, should report directly to the undersecretary for technology.

Need for an R&D function that serves all the responsibilities of the department.

Each division should have unambiguous and distinct operational roles, and each should have its own R&D capability in support of those operational responsibilities. This R&D should be designed primarily for identifying needs, evaluating solutions that are offered, and doing the actual procurement, and managing the deployment (often in collaboration with other federal agencies, with industry, or with local government). The budgets for all of the R&D in the Department should be the responsibility of the undersecretary for technology, but the R&D capabilities in support of the operational responsibilities should be managed by the division executives.

There should also be a central R&D function headed by a Director of Research reporting to the undersecretary for technology. It should not be managed by one of the operational managers who have to decide how to split their R&D resources between their own division's priorities and those of other divisions, as suggested in the President's bill. A council chaired by the undersecretary for technology comprising the director of research and the senior technical manager from each of the divisions would be a useful mechanism for collaborative planning and program coordination.

Adapting the President's bill to meet these needs

I see no way to avoid asking Congress for an additional high level position (undersecretary) for the chief technology officer. This will be a hard job to fill well; the incumbent will have to command the respect of the operating executives and have good enough access to the Secretary to force decisions to that level when necessary.

Stepping back from the President's bill as it stands, the problem of the mixed operational and support functions in most of the divisions is best met by restructuring the department into one group of units providing support functions – analysis, strategy setting, acquisition and forensics and intelligence – and a second group of units with primarily operational responsibilities – border control, hardening targets, deploying tools, response to attack and services for recovery. These two groups might be managed two under or deputy secretaries. But I acknowledge that this is not a "green field" management creation; agencies come as they are, and it will be hard to dismantle and reconstruct them while they are adapting to their new missions. But if something approaching this cannot be done, the Department will not look very different from what we have now, except for a unified management chain at the top.

Homeland Security activities outside the Department

Finally, one last point: the full architecture of the S&T response to terrorism must include important research activities outside the new department. A properly staffed Office of Homeland Security in the White House, working with the Office of Science and Technology Policy, is essential to take leadership for defining the responsibilities in DOD and in other agencies outside DHS for contributing to homeland security. There remains the question of how these external services can best be obtained. There are three alternatives: bring the capabilities into the DHS (certainly not practical), bring the other department or agency's funds into DHS and then have DHS repurchase the services from that department or agency (which I believe the President's bill intends as the way to access NIH services), or create requirements by the DHS to which non-DHS agencies and departments are encouraged to respond in their own planning and budgeting. If the Office of Homeland Security in the White House is strong, and is supported by OMB and a strong OSTP, this third alternative is the mode of choice in my view. I am very concerned that the repurchase approach will lead to micromanagement and a diffusion of responsibility. This system prevails in the way DOE relates to its national laboratories, and is widely criticized. It should not be emulated in the new Department if it can be avoided.

In closing, I would like to thank the committee for their invitation to testify and for the opportunity to share these views. Now, I would be glad to answer your questions.

---

[1] *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academy Press, available in PDF on line at <http://books.nap.edu/html/stct/index.html>.

[2] In the Academies Report, and in common usage, "critical infrastructure" includes all the commonly understood infrastructures – energy, information, transportation, food systems, health systems and cities – thus most of the scope of the *entire* department. But in some government documents, "critical

infrastructure" is taken to mean only IT infrastructure.

[3] See Chapter 12, pages 12-7 through 12-9 in the prepublication copy of *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*.