Minutes

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security Science and Technology Advisory Committee (HSSTAC) in Arlington, VA November 15-16, 2004

The Homeland Security Science and Technology Advisory Committee (HSSTAC) convened its fourth meeting on Monday, November 15, 2004, in Arlington, VA. The Committee opened in closed session pursuant to the provisions of 5 U.S.C. 552b(c)(9)(B).

The Designated Federal Official, Dr. Ronald D. Taylor, called the meeting to order and, per the Committee's charter, turned the conduct of the meeting to the Chairman, General Larry D. Welch, USAF (Ret.). General Welch reviewed the objectives of the meeting, reminded members that the Committee's initial annual report is due to the Under Secretary and then to Congress by the end of January, and also reminded them that the next meeting of the Committee will be on February 23-24, 2005, in Washington, DC. As announced in the Federal Register (69 FR 61855), the meeting objectives were: (1) to receive briefings from its subcommittees on recent activities and findings in support of the annual report to Congress; (2) to deliberate subcommittee findings and provide recommendations to the Under Secretary; and, (3) to determine any future Committee actions. General Welch noted that on the first day the Committee would hear from each of the four Subcommittees: Mission & Operations, Resources & Organization, Programs, and Outreach. On the second day the Committee would discuss its findings and recommendations and would meet with members of the public in open session to provide an overview of its work and solicit their views.

Under Secretary for Science and Technology

Dr. Charles E. McQueary, Department of Homeland Security Under Secretary for Science and Technology, then delivered remarks to the Committee. Dr. McQueary thanked HSSTAC for being an important resource for the Science & Technology Directorate (S&T) as it defines and pursues its research, development, test, and evaluation (RDT&E) mission. Since the last HSSTAC meeting on August 31 – September 1, 2004, the S&T Directorate made advances in several key areas.

Last month the S&T Directorate initiated its FY 2007 – FY 2011 planning, programming and budgeting cycle. This cycle and supporting planning process implement new procedures for making decisions about meeting S&T's RDT&E programs. In this process, S&T will use a risk-based approach for its planning. Also, in accordance with requirements of the Homeland Security Act, S&T is coordinating with

federal agencies in preparing a government-wide National Policy and Strategic Plan for homeland security.

In September, S&T joined its partners at the National Labs to dedicate the Biodefense Knowledge Center at Lawrence Livermore National Lab. The Biodefense Knowledge Center is the first of its kind in the United States and will serve as the hub for the nation's biodefense expertise and will enable collaboration and data sharing among scientists, policy makers, first responders, analysts, and law enforcement officials.

The S&T Directorate continues to build the network of Homeland Security Centers of Excellence. The next Center of Excellence will study the behavior of terrorists and the social effects of terrorist threats and attacks on society. Two other Centers of Excellence that are addressing aspects of bioterrorism are already operating. One of these, located at Texas A&M University, is studying high-consequence foreign animal and zoonotic diseases. The other, at the University of Minnesota, is working on food security. Both of these Centers have ties to the National Center for Risk and Economic Analysis of Terrorism Events at the University of Southern California – which is developing and applying tools for assessing the risks, including consequences, of terrorism.

Last month the S&T Directorate announced the Department's first international biometric facial recognition standard to use in verifying the identity of foreign nationals entering the United States. Developed in coordination with the private sector, the standard will assist federal agencies, state and local officials, vendors, and travelers in order to produce photographs that will be accepted in new passports issued by the State Department. This standard will help define photographic properties, digital image attributes, and a standard format for applications. This new standard is intended to facilitate information sharing among intelligence agencies.

Other advancements include work done by S&T's Homeland Security Advanced Research Projects Agency (HSARPA). HSARPA currently has five active Broad Agency Announcements (BAAs) on a variety of topics. These topics include personal protective equipment for emergency responders, cyber security, chemical detection systems, and unified incident command.

The Scholars and Fellows program is an example of how S&T continues to contribute to the government-wide effort to build U.S. scientific leadership. This past weekend S&T welcomed the newest class of Scholars and Fellows at an orientation in Washington. The program currently has 175 undergraduate and graduate student participants studying in areas directly relevant to homeland security.

In closing, Dr. McQueary thanked the HSSTAC members for their efforts with the S&T Directorate and for their service to the nation.

Mission & Operations Subcommittee

Dr. Richard Roca and Mr. Vincent Vitto, Co-chairmen of the Mission & Operations Subcommittee, briefed the Committee on the Subcommittee's findings and recommendations regarding the S&T strategic planning process. Other members of the Mission & Operations Subcommittee present were Ms. Lillian Borrone and Sheriff Ted Kamatchus.

As reported, the Subcommittee had met twice to gather information and formulate its ideas. Input was received on August 17th from members of the DHS staff responsible for the following areas: process and methodology used to establish mission and strategic goals, the approach to threat identification and prioritization, the process used to establish budget priorities and investment strategies, and the FY05 and projected FY06-10 budgets of the S&T Directorate. On October 19th the Subcommittee met with the portfolio leaders and teams responsible for threat identification and prioritization, as well as representatives from the Homeland Security Institute.

The Subcommittee discussed the following: (1) the need for the S&T Directorate to clearly define its strategic goals and objectives with associated metrics to guide both planning and budget prioritization; (2) the need to consolidate threat characterization and vulnerability assessment activities; and, (3) the need for S&T to develop a process to transition mature RDT&E products and capabilities to other operational entities outside the Directorate.

Programs Subcommittee

Dr. William Happer, Chairman of the Programs Subcommittee, briefed the Committee on the Subcommittee's findings and recommendations based on briefings from the Biological, Chemical, Radiological/Nuclear, and High Explosives Countermeasures portfolios. Other members of the Programs Subcommittee include Dr. Ronald Atlas, Dr. Kenneth Shine and Dr. David Franz.

As reported, the Subcommittee met twice to gather information and formulate its ideas. Input was received on August 9th from the Biological and Radiological/Nuclear Countermeasures portfolios; and on October 7th from the Chemical and High Explosives Countermeasures portfolios.

The Subcommittee discussed the following: (1) the need to engage and leverage relevant work in other Federal agencies; (2) the need to engage across all sectors of Federal agencies, state and local governments, and the private sector to work for dual-use purposes; (3) the need to ensure that early warning and surveillance programs strike a balance between near-term product improvement and deployment and more effective protection in the future; and, (4) the need for a rigorous, independent, and unbiased peer review process that assesses program execution, mission relevance, and scientific and technical quality.

Resources & Organization Subcommittee

Dr. Alice Gast briefed the Committee on recommendations and findings pertaining to the resources and organization of the S&T Directorate. Members of the Subcommittee include Dr. Larry Papay (Chairman), Dr. Alice Gast and Chief Joe Polisar. Dr. Baruch Fischhoff also supported the Subcommittee and participated in the analysis. Discussion focused on the following: (1) what S&T budget level would be appropriate to anticipate and support future demands of the Directorate; (2) sustaining S&T's budget while facing increasing demand to support operations; and (3) consolidation of the Department's research & development efforts.

Dr. Papay then briefed the Committee on the specific results of the Subcommittee's work that examined options whereby the S&T Directorate (and the Department) could, over the long term, access the scientific and technical capabilities resident in the Department of Energy National Laboratories.

The Subcommittee met four times to gather information and formulate its ideas. DHS Office of Research and Development, DOE Office of Science, the National Nuclear Security Administration and Field Offices, current and former staff from the DOE National Laboratories, Management &Operating contractors, and other experts provided inputs to the subcommittee.

The Subcommittee focused on identifying a process (sequence of steps) by which DHS could develop a sustainable program with the laboratories. Dr. Papay described the various forms of contracting with the National Labs as set forth in the enabling legislation: Joint Sponsorship, Direct Contract, Work for Others and "Any other method approved by law." Dr. Papay explained the Congressional mandate for the S&T Directorate to manage and oversee all DHS-National Laboratory relationships and went on to discuss: (1) the need for S&T to more clearly define the needs to be met by the Laboratories, and (2) the specific approaches that could be used to meet these needs. Approaches ranged from engaging laboratories under the existing Memorandum of Agreement (with DOE) to creating cooperative agreements with multiple laboratories.

Outreach Subcommittee

Dr. Russell Bessette, Chairman of the Outreach Subcommittee, briefed the Committee on the Subcommittee's findings and recommendations. Members of the Outreach Subcommittee include Dr. Baruch Fischhoff, Chief Ernie Mitchell and Mr. Tony Ibarra. The Subcommittee discussed: (1) the Department's need to build resilience in the public with an effective public awareness campaign that addresses prevention, reaction and recovery; (2) the need for DHS to gather input to stimulate science and technology from first responders who are concerned with preparing for and managing real alerts and attacks; and, (3) the need to continue to involve small businesses and non-profit organizations with the development of technology.

The first day's session adjourned at 4:00 p.m.

The meeting reconvened at 8:30 a.m. on Tuesday, November 16, 2004, in Arlington, VA. General Welch discussed the requirements and format for the Committee's report to Congress due the end of January, and set deadlines for members to provide final input to the report by the first week of January. The Committee then discussed its findings and recommendations consolidated from the first day's briefings.

The closed session ended at 9:45 a.m.

Public/Open Session

The Committee reconvened at 10:10 a.m. in open session. Following is a transcript of the open session.

GENERAL WELCH: I'm Larry Welch, Chairman of the Homeland Security Science and Technology Committee and to my right is Dr. Charles McQueary who is the Under Secretary for Science & Technology of DHS. This Committee is a federal advisory committee mandated by Congress in the Homeland Security Act of 2002, comprised of 20 members with very broad and varied backgrounds.

The Homeland Security Act of 2002 requires us to submit an annual report of activities and recommendations via the Under Secretary for S&T to Congress. The Committee meets in plenary session once a quarter. Most Committee work, though, is actually done by its subcommittees.

The Committee is comprised of four subcommittees: Mission and Operations, Programs, Resources and Organization, and Outreach. At the plenary sessions, the Committee reviews their work and discusses where we are and where to go.

We spent all day yesterday and part of this morning discussing in some detail the formulation of findings and recommendations for our annual report. We'd like to remind you at the outset the magnitude of the task that faces the Department of Homeland Security. Simply bringing together 22 agencies into a single department is a monumental task, particularly since every one of those entities has to continue to perform everything it did before entering the Department. I sometimes remind people it took more than 50 years to bring the War Department and the Department of Navy together. It may take a while for all of this to come together into a smoothly integrated department. Nevertheless, we see impressive progress. And, while there is much work remaining to be done, we are providing advice on their work.

Obviously, since we are in the process of producing a draft report to Congress, we won't be providing you with specifics about our recommendations, but I will give you an overview of our findings and recommendations.

At the head of the list, not surprisingly, is the need to define clearly and communicate widely the strategic goals, objectives, and planning for the programs that

support the needs of homeland security. We are not saying that the Department does not have strategic goals and objectives *per se*, but that they need to be "actionable" and they need to be communicated very widely so that they serve as guides for what people do in the Department every day. That's always a challenge for any large department and certainly a particular challenge for a department made up of as many diverse activities as this department.

A second area that has been clearly assigned is responsibilities for a very complex set of demands within DHS and within the S&T Directorate. We find the need for a process for transitioning products and capabilities from RDT&E to operations. That's particularly complex because we're talking about filling a set of capability needs that are being developed. It's a moving train, and every day new understanding, new knowledge of what it really takes to provide homeland security, is very much evolving with not a lot of reliable history on which to depend.

Along with that we see a need for metrics to help determine how much is enough; that is, how far should one go in each area before shifting resources somewhere else? A major issue is how to transition from simply focusing on individual threats to focusing on the vulnerabilities created by a set of possible threats. The reason, of course, for that focus is that we'll almost always be wrong about individual threats. Nobody has enough intelligence or enough information to predict with any kind of accuracy that a specific threat will materialize in a specific place within a specific period of time. The challenge is to characterize a wide set of threats so we can identify vulnerabilities and take action to close or mitigate those vulnerabilities. So regardless of how the threat develops, you have a more resilient society and more resilient capability to deal with threats.

We see a need for a well-defined and orderly process from seeking solutions to fielding capabilities. This challenge is made more difficult because there is not an established industry to look to for solutions to homeland security needs. There is instead a very wide range of small businesses, universities, and big businesses, and a wide range of approaches and resources for defining and delivering solutions.

We see a need for closer interface with other federal agencies, because homeland security depends on cooperation with a wide range of agencies -- the Department of Defense (DOD), the Department of Energy (DOE), the Department of Health and Human Services (HHS), the Environmental Protection Agency (EPA), the Department of Agriculture (DA), just to name a few. So the interagency demands for interaction are particularly challenging for this particular mission.

We see a need for specific programs both that define the near-term and the long-term mission needs -- how one transitions from product improvement and delivery to help first responders and others deal with consequences and vulnerabilities, and the need to commit research and development and S&T to longer term solutions that are more complete.

And finally, we see a need for a peer review process that ensures independent and unbiased judgment are brought into assessing program execution and research and technology development, etc. Again, this is because we're talking about such a broad range of technologies provided by a wide range of entities.

There is a need to establish a set of relationships that leverages the expertise of the National Laboratories. Given the variety of National Laboratories and the variety of needs, there needs to be a variety of relationships. You need not dwell on the fact that there are always political considerations involved there and the relationship needs to be not only with National Laboratories, but also with other government laboratories, universities, small businesses, and nongovernmental organizations. Again, we see a very broad set of relationships.

Finally, we see a need to define and execute an outreach program that contributes to the resiliency of the public in general. We all know that the effects of a particular attack on the public go far beyond the actual physical effect. The effects are very much mitigated or exacerbated, as the case may be, by how well prepared the public is to deal with it, how the public sees the government response, be it a city, a state, or the federal government.

How to prepare the public without unduly alarming them is a very complex task that requires a level of understanding of public policy and psychology of disasters, etc., and one of the areas where we will have specific findings and recommendations.

There are other findings and recommendations, but I think that's enough to give you good insight into our work and our thinking and where we see significant needs and the kind of advice we are offering the Under Secretary.

We are available to respond to your questions, to discuss subjects you would like to discuss within the constraints of this Committee meeting, and to talk about a draft report to Congress. With that, we're open for discussion.

MR. DETTER: I am Brian Detter from the University of Nebraska Medical Center. What are the four subcommittees?

GENERAL WELCH: Mission and Operations, Programs, Resources and Organization, and Outreach.

MR. EPSTEIN: I'm Gerald Epstein from the Center of Strategic and International Studies. It seems one of the toughest jobs the Department has is prioritizing things that really are impossible. Did your Committee look at that and how the Department should deal with different threats?

GENERAL WELCH: As we have already stressed, we think you have to be able to move beyond individual threats to sets of threats and identify vulnerabilities and a set of balances. One is the consequences of someone exploiting vulnerability. That's much

more productive than trying to predict that the al Qaeda will attack a building in Chicago or al Qaeda will do something somewhere else. There is a set of priority choices that we will have some recommendations on, or at least, some processes for dealing with them. There are priority choices across portfolios. There are priority choices across dealing with vulnerability to a biological attack, vulnerability to a radiological attack, and so on.

And the priorities are influenced by the vulnerability by the availability of some kind of solution. There has to be some concept of how one might make progress in dealing with things that are very high on the priority list. There is always the balance between what you can deliver today that will help, and the resources necessary to commit to what will be delivered several years from now that may be more effective.

So there is a whole set of these balance issues that have to go into priority decisions. While we don't make specific recommendations about specific programs, we have findings and recommendations on processes for making those priority choices.

MR. RAO: Ganesh Rao, with Underwriters Laboratories. Would you speak about initiatives underway on cooperating with other federal agencies?

GENERAL WELCH: I think I should let Dr. McQueary answer that.

There are times when interagency cooperation works very well, and there are times when even with very well established missions such as the Department of Defense, where we've been dealing with these issues for decades, we still find ourselves with serious shortfalls in the interagency process.

There are processes -- mechanisms -- that are set up. DHS, in the view of the Committee, has a particularly challenging set of issues. With a biological attack, or a chemical attack, or a radiological attack, DHS must work with HHS and EPA, and these people have resources and responsibilities that DHS has to interface with. If it's a nuclear matter, DHS interfaces with DOE. For conventional explosives, they have to interface with DOD. If it has to do with agricultural vulnerabilities, DHS deals with the Department of Agriculture. So the Committee is in a position at the present time of telling a mouse to fly, but we can't quite tell him how to fly.

I think the Department has put an enormous amount of energy into establishing these interagency relationships. When there is a crisis, these relationships seem to develop relatively fast, but that's not the approach people want.

DR. McQUEARY: I think you summarized it very well, but I would say that we do have a well-defined process if we have an emergency condition such as going to Code Orange. Our Homeland Security Operations Center, an interagency management group, is well-defined and has specific people with specific roles, but there is an aggregation that takes place to draw upon people from all the relevant agencies in a

time of crisis, to advise the Secretary on what decisions could be made based upon the circumstances. I feel pretty good about how that's working.

Obviously, we have not had a real crisis to test this, but we've had elevated threat levels. We exercise the system through what we call “Top-Off” exercises to see how well we respond and to identify problems so we can fix them.

MR. MacBAIN: Jim MacBain, University of Michigan. What is the process that you have in place today for uncovering the most promising but long-term ideas such as explosive detection devices? The threat seems to be all over the place and, well, just what do you have in mind for that?

DR. McQUEARY: I will ask Vayl Oxford, who runs the Homeland Security Research Projects Agency, to respond to the question.

MR. OXFORD: We actually do that in three separate ways. We do it through the Small Business Innovation Research (SBIR) program where we look for innovative ideas in a variety of categories and those are generally open to selection topics on a biannual basis. We are doing it through direct solicitations using Broad Agency Announcements (BAAs). We are also very active with the Technology Support Working Group (TSWG) that is looking at specific applications, such as countering the Improvised Explosive Device (IED) problem in Iraq. We look at that as an opportunity for joint ventures on explosive detection of domestic threats. So there is really a three-pronged approach: direct solicitations out of our explosives program; the SBIR program looking at the longer term solutions where innovative ideas may take us past the current solutions; and interaction with the TSWG.

DR. McQUEARY: We also have had a number of interactions with international allies who have a great amount of experience in that area.

GENERAL WELCH: Let me say just a word about the Committee's view on the need to advertise or to inform more broadly the tens of thousands of small businesses, universities, and others of new ideas and solutions to difficult problems.

One of our suggestions is that we widely inform this particular group of people whenever a new BAA or a new Request for Proposal (RFP) appears on the web site. This would simply increase awareness of how this process works within the Department. The process is working, reaching out to the thousands of entities that can contribute new ideas.

DR. McQUEARY: If I could just add a point to this, the issue ultimately gets back to what we are trying to do because even in the case of explosives, there are techniques that we've seen that could actually blow a person up, to put it bluntly, depending on the type of explosives. Is that the kind of capability we want to field in this country or do we prefer simply to detect?

You can analyze a range of what we need to look at, and I think our role is to help answer questions in all of these areas. We've got to determine what the command and control feature is going to be that goes with that piece of information and how to collect this information, and the network to provide the requisite information to whomever it is that needs to be able to make the ultimate decision. So while we spend a lot of effort on detection, which is an important part of solving the problem because if you can't detect you can't do the rest of it, the larger problem is the architecture of how we put all of this together.

MS. POULAKIDAS: My name is Jennifer Poulakidas. I'm with the University of California Federal Relations Office here in Washington. There have been a few changes recently in the leadership of cyber security at the Department, and I'm curious if you might be able to share the Committee's wisdom and advice on the future of cyber security within the Department. Perhaps you have recommendations about where cyber security should be housed or if it should be housed in multiple directorates, any information you would be willing to provide.

GENERAL WELCH: It is hard to think of a subject that is more entity-specific than cyber security; that is, cyber security is everybody's business. We note the rapid development of cyber security awareness but willingness to take cyber security action is, by and large, a business decision. We have seen the finance and banking system move from the attitude that they don't want to advertise cyber security problems because it hurts their brand name, to the attitude that cyber security is not a threat to your brand name -- it's a threat to your business. So they must take it seriously.

No one has been successful in prescribing cyber security standards that have any real meaning from any kind of a central authority simply because of the very widespread entity-specific issues on cyber security. Most of it is in the private sector. On the other hand, you can set standards and policies that you have to meet to get on somebody's network, and that's the approach that the Department of Defense uses, for example.

But in answer to the question of who should be the entity in charge of “National Cyber Security,” my answer is that I can't imagine how one does that. What you can do is have a massive program of awareness, and it appears that is going on.

DR. McQUEARY: As you know, the cyber security division is located in the Infrastructure Protection unit, and it is my view that that's where it should be because the web is really a part of our critical infrastructure. To put it in some other location when we've got an organization that is dedicated to identifying the vulnerabilities and helping the satellite defense to be done, would not be a good organizational decision.

So the responsibility is where it is and that's in the Information Assurance & Infrastructure Protection (IAIP) Directorate. The Science & Technology Directorate actually has a R&D responsibility to support them. In particular, we funded a joint effort with the National Science Foundation to build a self-contained web, if you will, at the

University of California Berkeley in which people can go and test systems to see whether they actually can improve or decrease the vulnerabilities, and also try to understand through hacking techniques what the vulnerabilities are so the systems can be made more robust.

In that sense, the Science & Technology Directorate has a supporting responsibility. It is my view that the discussion about the level of the person that runs it is somewhat of a red herring, because I've seen very effective organizations operated by people well down in organization. You must have somebody who knows what they are doing, in particular, where they reside to guarantee success or failure. You must have the right people in the position.

GENERAL WELCH: I might add that you can inform, but you can't direct execution. Most of critical infrastructure is private and their decisions are business decisions, but the informing role is an extremely important role, and there does seem to be a fairly good response to it.

DR. McQUEARY: I agree with the point General Welch made about most infrastructure being owned by the private sector -- particularly the cyber -- and it being a private sector issue. This administration is not in the mode of trying to put in place more and more regulations.

If we can move this along enough so the issue of cyber security or any other physical security that might be added to it for companies becomes a competitive issue, my personal view is that people end up doing the right thing, because all we have to do is have a few companies making themselves more attractive on Wall Street. They make it known that we've done the things that really make it a more secure investment for your money, and then other companies will follow. We don't have that loop yet, and to me that would be an ideal kind of solution for this country because that's what we're all about.

We want businesses being successful and addressing general security issues within the competitive environment; and if we have people and businesses do the right things on their own as opposed to having the federal government say you must do this or that, then the country would be far stronger and more resilient.

MR. SMITH: I'm Toby Smith with the Association of American Universities. I want to comment on the mechanisms for interagency coordination because I see in the university community a large frustration that there isn't better coordination, especially since our community really wants to provide help since 9/11.

Is the Committee going to look at an actual interagency mechanism, not just in an emergency situation, for coordinating what's happening as it relates to both short-term and long-term needs in homeland security? I don't see that entity existing, and I think it would be very helpful.

It's also important to consider not just coordinating the interagency efforts, but also the agency's outreach efforts especially to the research community. I would point toward some efforts for large scale initiatives. For instance, in nano technology there is an interagency council and a central office, and you can actually go to a central web site where you can find if there are agencies in a particular area that are holding conferences or if RFPs are being issued. It would seem even right now within the Department of Homeland Security that you have different parts of the S&T Directorate issuing BAAs at different locations on web sites.

So, some type of coordination, both in the Department as well as interagency, would be tremendously helpful to the external community as well if that could then be represented through some effort.

MR. OXFORD: Let me address that in two different ways. First of all, we are proactive on the interagency side in that we work a lot with existing structures; however, we should not set about creating an interagency process unless we have to. We are active in the National Science & Technology Council. In fact, Dr. McQueary is one of the co-chairs of that group along with Mr. Wynne from the Department of Defense and Ms. Dale from Office of Science & Technology Policy (OSTP). They have a committee structure that deals with some of the issues that you reference.

We also deal with another White House group called the Counterproliferation Technology Coordinating Committee that does interagency coordination in chemical defense, biological defense, and some other issues that aren't as directly relevant to DHS.

When you talk about the outreach program, we understand that our web site has not been as useful as it should have been. We hope to see a major change in our web presentation and its utility in a few weeks when you will get a lot more visibility into the BAAs that are coming out. This outreach program will start to take a lot more root than what you have seen over the last 20 months. We recognize the shortfall.

GENERAL WELCH: It's useful to remind you, of course, that DHS brings together 22 separate organizations from multiple departments into a single department. That phenomenon in and of itself is a massive step towards forcing better interagency coordination.

MR. EPSTEIN: I want to ask about international cooperation. Are we looking at coordinating research with international partners? Are we looking at barriers? Are they making it hard for us to tap people over there?

DR. McQUEARY: The answer is we have a number of ongoing efforts and several things have happened so far. We have a signed agreement with the Canadians at this point on technical interchanges on issues related to homeland security.

We are nearing completion of an agreement with the British that we expect to have finished by the end of the year.

We've had discussions with the Australians which will probably be one of the next places we would go. We've had discussions with the Japanese and the Israelis, discussing agreements with them to exchange technical information as it relates to homeland security issues.

DR. McQUEARY: I have a question for you [the public]. I notice we have a number of people from universities. I'm a little curious as to what prompted your interest in attending the session this morning, if you wouldn't mind telling me.

MS. POULAKIDAS: Personally, I just think that we're all starving for any kind of inside information from the S&T part of the Department.

I think I can speak for myself and for some of my colleagues – we have great interaction with some of your staff, but any more information we can get is always helpful, so thanks for this opportunity.

MR. MacBAIN: Just adding to that, there's been tremendous interest in the university community in the S&T Directorate itself. So I think part of the reason you see a lot of people here is we are just trying to look for opportunities in which universities can be helpful.

GENERAL WELCH: Is the university community generally aware of the availability of information on the DHS web site or on the S&T web site? Is it something that is just virtually unknown?

MR. MacBain: I can only speak for the University of Michigan. My job is to look for mainly engineering research opportunities. We know about the web site, but the BAAs that show up now and then are few and far between. They're also very broad. We don't know if they're for universities, or for a Lockheed Martin, or how we fit in. People don't want to spend a lot of time preparing proposals if it's all going to be applied and doesn't fit the solicitation and it is not always clear.

Faculty members come to me with what they think is a good idea. If there is no direct BAA, the only thing I can offer them is the TSWG competition, and that strikes me that everybody from a postman in California to some scientist in Connecticut can apply to that.

I have a sense that there must be piles of proposals somewhere here in Washington. I'm not sure whether the good ideas see the light of day. So that's the impression we get. And there are the SBIR proposals. We'd love to work with small businesses, it's a great technology transfer tool, and we follow those with the different agencies.

MR. SMITH: It's confusing at this point. We don't know for sure where we fit. We really want to fit. We have tremendous capabilities across the country to help meet these solutions. Yet we don't feel like we have a way to do it.

There is the Centers of Excellence program you have, but do you have individual investigator solicitations? Do you have small groups? I don't think so at this point.

DR. McQUEARY: Actually, we have all of the above. I'll say it the following way: We have a pretty good view of what we need to do and, therefore, the BAAs have been a major mechanism for us to get ideas. This is what we are interested in.

This is not to say we have no interest in independent solicitations. Although we have put a lot of effort and thought into where we have holes in the scientific work that needs to be done to support the Department today, we don't find a lot of what I'll call "basic research" and the reason for that is very simple. It was a decision I made early on when I got into this job -- that we have too many problems that need to be dealt with today in the Department to spend a lot of early effort in what we normally call "basic research."

What we expect to happen over time is that there will be a shift in balance between the problems of today to eventually where we're really working on research. It was my conclusion that if we started out with a heavy research component for the Directorate, our output was going to be five or six years downstream. In all likelihood if it was doing research work, then the rest of the Department would go on and do its job and we wouldn't have any relevance.

So I concluded after a lot of discussion with senior staff that we must do things that are important to this new Department to establish our *bona fides* so that we will be looked upon as a resource, not just a research group doing something that's not relevant to the work that needs to be done to meet our mission.

We are admittedly in a transition phase, and it's all tied together with what I call the basic systems with the job we've got. We have a set of circumstances and characteristics that define what our homeland security capability is today. I believe it's possible to set the vision and that's a job that we have in S&T. Where is the vision that we need to get to? The hard part of the problem, quite frankly, is how to go from here, where we are today, to where we need to get to. After you get there, evolution is really easy comparatively speaking. But the hard part is making both evolutionary and revolutionary changes to where we need to get to without upsetting the flow of commerce and visitors to this country.

So it's just like the analogy of changing the wings on the plane while you're flying. It's a hard problem to be able to do that. But we have a lot of capable people, and I'm confident that we will be able to do that.

MR. OXFORD: One thing that I'd like to address is the question about whether these are Lockheed Martin kinds of contracts or contracts for other kinds of organizations. Congress gave us something called the “Other Transaction Authority” capability which allows us engage the small business and academic communities.

So when we go out with the solicitation, we are open to whatever type of contract we may need to award based on the capabilities of that entity. We have actually awarded a lot of contracts to universities through the “Other Transaction Authority” process. So it's not always a direct FAR contract that we're awarding. Our approach is predicated on this flexibility to try to engage the academic community and others, but it's very flexible.

GENERAL WELCH: Following up on the questions from the University of Michigan representative. You mentioned “basic” versus “applied” research. Do researchers really care whether it's categorized basic or applied?

MR. MacBAIN: Well, from an engineering perspective, I would argue a lot of our research activity is applied, and so we do a lot of partnerships with industry. I think we're further along your R&D spectrum than, say, a physics department.

So I really feel like we could contribute to the applied needs because we already do that. One piece of advice I give is to look at NIST’s Advanced Technology Program (not a popular program in some areas now), it's an industry-led activity, but they encourage university partnerships. That's an excellent technology transfer tool, and we know that what you want to do is get something working. You're not interested in funding research for research sake, so that's something to consider about encouraging university/industry partnerships.

GENERAL WELCH: A group I was involved with just finished a National Research Council (NRC) Study on DOD Basic Research, and one of the universities we interacted with was the University of Michigan. We discovered that many researchers have no idea whether they're doing basic research or applied research, and they couldn't care less. They care about the interesting work and the ability to sustain funding to continue.

MR. SMITH: I think there are still some cultural issues. A lot that has been done by the Department has been oriented towards industry, so I do think some of our universities are having trouble going to conferences, and things like that, which seem somewhat foreign.

Actually there also are issues with universities with regard to “Other Transactions Authority” which I won't go into here, but they have to do with concerns about intellectual property rights.

I'm very pleased with the University Centers of Excellence Program. The one question I have is how the university centers -- they're in the crosscutting portfolios that look at various threats -- fit with those various portfolios since they are not a part, or

they don't seem to have a natural stream or feed into the various portfolios, that you outlined that are along the thread of vulnerability.

DR. McQUEARY: Well, we're looking for the universities to help define the areas of research. In fact, the process is a grant process for all practical purposes. We specifically did not enter into contracts with them to produce a certain thing. We entered into an agreement that they would work in the area generally defined, and the universities themselves will help define what those programs are going to be, obviously subject to our approval.

They are intended to be crosscutting; they are not intended to be assigned to specific portfolios, although some will match up more closely than others. The way we arrive at which university we should have is that we get senior leadership within S&T together and they come up with a series of possibilities and we develop recommendations.

We then try to go out to the operational units within the Department to be sure that what we're going to do is viewed as being helpful to the operational units; because if they all say: "We don't care anything about that," then the question arises, why are we doing it?

From there, the recommendation ultimately comes to me, and I'll either agree or disagree. There are people who have done an excellent job in making choices, and I have not disagreed with a single recommendation that has been made so far. That is the general description of how we intend to use them. This is unplowed ground to a degree, and we are learning how to use them as we go along. I don't have a precise answer because if I knew the answer, then we probably wouldn't need to hire a university or anybody else to help us work through the answer. We are looking for an increased knowledge base that can come about as a result of having people do research in these areas that we've identified.

MS. CAMPION: My name is Moira Campion. I'm with New York University Federal Policy. I would like to hear more about the Committee's view to broadening Homeland Security's thinking regarding sets of threats across an entire industry or community as opposed to specific threats (for example, a threat to Citibank). What are you using to guide your thinking on this and how might you envision your recommendations to Homeland Security within the next few months being implemented?

GENERAL WELCH: There is a general broadening of the understanding of the difference of the world that we live in today compared to the world that a lot of us grew up in. Formerly, it was useful to focus on capabilities *vis-à-vis* a specific threats like the Soviet Union or North Korea, etc., but we don't live in that kind of world anymore. We live in a world now where a wide range of entities have the capability to do serious damage to the U.S. structure and U.S. society. I think that we as a nation are having difficulty conceptually changing our thrust.

Within the Department of Defense, the approach has been to go from threat base to capability base. It's the same concept. That is, we can't define what sets of threats are the most likely to occur in the future, so we simply describe a range of threats used to define the needed capabilities to ensure that wherever the threat develops, whatever form it takes, that we are prepared to deal with it.

I think we are talking about the same approach here. That doesn't mean specific threat warning is not useful because the real purpose of specific threat warning is to raise awareness, to raise preparedness, to make American citizens more vigilant without making them paranoid. In the end, I don't think any of us expect that we're going to be able to identify in a specific period of time that a particular group is going to do a particular thing in New York City, Chicago, Los Angeles, or Iowa.

So we are forced to look at broad sets of threats and assess the vulnerabilities. The vulnerability you want to be the most secure against is any set of threats having the ability to disrupt the fabric of U.S. society – the U.S. way of life - and from that you come down to specific things that could really strongly disrupt that fabric. You can name them as well as I can.

If one could seriously disrupt the banking and finance industry, it would have enormous impacts on the fabric of the nation. You can go through a whole series, such as transportation systems. So then instead of trying to devise defenses against just smallpox, or trying to design defenses that keep people from driving airplanes into buildings, all of which are highly desirable, you have to address how can you reduce vulnerabilities, and there are multiple aspects to that.

One aspect is how to reduce the actual physical damage, how to mitigate the loss of life. But equally important is how to ensure the public can deal with it. How you ensure that the public will retain confidence in the government is also relevant to address. I would give you the example of 9/11.

My point is that by dealing with vulnerabilities, you don't have to pretend that you can identify a specific threat, at a specific time, against a specific target. Instead, you use those kinds of insights to define the vulnerabilities at each level, to ensure that none of those things can seriously disrupt the fabric of our lives.

They can kill people and that's bad. The fact is that while disasters are terrible, if handled properly and if the public is prepared and knows how to respond, they don't do serious damage to the fabric of this society.

So that's kind of a long-winded answer, but this is not a concept that applies just to DHS. It's a concept that applies to DOD and DOE because all of these organizations have had to deal with the fact that we live in a very different world where the threats are much more diverse and much less predictable than the world that I spent 70 years in.

MR. VITTO: When you look at this approach to vulnerability assessment, you can see there has been a lot of work done in the public sector on identifying vulnerabilities, for example, to the power grid. One of the interesting and really complex scientific thrusts is the whole interrelationship between infrastructure correlations, as we saw in 9/11: transportation, banking, finance, and all sorts of interrelationships. So the whole complex modeling of interrelationships between infrastructures is going to be something that will require a great need for the best and finest analytic minds in the nation to bring to bear.

It's not just a static analysis, it's a dynamic analysis, and there are no theoretical frameworks at this point that I know of that truly address that. So this is an area that the university community, the National Laboratories, and others should be focusing their attention on because if we do take this vulnerability approach, which is the important way to go as General Welch has pointed out, it's not enough to isolate one infrastructure or one domain. One must understand the complete interrelationships between the domains.

GENERAL WELCH: And by the way, DHS S&T has some initiatives in this area.

MR. DETTER: Two quick questions. First, when do you expect the report might be issued? Second, about 10 days ago, there was an interesting article in the *Washington Post* about bioterrorism and both the progress that has been made to-date and some of the hand wringing that's going on. I was wondering if the Committee has an eye on that. The article talked about detection capacity issues, and vaccine technologies, and I didn't know if the Committee had any comment.

GENERAL WELCH: The first issue is that the Committee's report by statute is for Congress so when it's released publicly is up to the Congress. But we will provide the report to the Under Secretary about mid-January and then the Under Secretary will provide it to Congress. I don't know how long that will take, I presume not very long. How long the Congress takes before they release it publicly is up to them.

So our obligation is to deliver a final report for calendar 2004 by mid-January 2005.

About bioterrorism, there is a whole set of issues in bioterrorism for which we don't have satisfactory answers. But if I were going to pick the single vulnerability area where we seem to be focusing the most intense resources across DHS, HHS, EPA, and DOE and a wide range of agencies, I would pick bioterrorism.

The reason that's particularly important is that we have reached a point where there is high confidence that we can deal with bioterrorism. It's not unusual for problems like that to lie on the too-hard pile for a very long time. This one is off the too-hard pile, and a lot of very bright people and a lot of very capable organizations are focused on dealing with these issues. So while we can all define some very complex issues for which we do not have answers, the good news is we have high confidence in

a lot of people that there are answers, and an enormous amount of effort is going into finding those answers, whether it be detection or treatment. Of course, one of the things about biological agents is that most of them are treatable. So you do have a layered set of defenses that can mitigate the consequences and prevent that from becoming catastrophic.

DR. McQUEARY: Certainly, the key element for us and the one we are spending quite a bit of money on is early detection. Of all threats that we deal with, the bioterrorism threat is the temporal, that is, time sensitive, threat. So it's very important to have sensors that can make early detection and provide the information, because when we can get early information, then we know how to do certain things to minimize the effect of whatever those things are that might be used against us.

By the way, the report that was written by the *Washington Post*, it's interesting to me that within less than a week's time there was an announcement that came out that HHS awarded a several hundred million dollar contract in vaccine-related areas to a company whose name escapes me. But a lot of these reports are written and sound terrible, because they don't recognize the work that's actually going on in preparation to address the problem.

MR. EPSTEIN: Under Secretary McQueary has a potentially very powerful new tool for homeland security, the Homeland Security Institute. Is this Committee providing guidance on how to use it or do you think you've got that under control?

DR. McQUEARY: It is a powerful new tool and, quite frankly, a very important tool. It's not just a tool for the Science & Technology Directorate, it's a tool for the entire Department, and we expect to use it that way.

For me the most important thing they are working on for us right now is the system architecture of this “thing” called homeland security. I think they have 25 or 27 different areas that they are working on, and they have begun to put some fabric around what I characterize as our number one problem: system architecture. They have begun to do some work in that area. We are not ready to go public with it yet because it's not far enough along to see that we've made enough progress to say it's good or bad, but the work looks encouraging to me.

So I'm very much interested and review on a monthly basis where we are with that work because I think it's really probably our most important contribution to the Department: how are we going to put all of this stuff together; what's the time frame; how much is it going to cost; how do you phase all of that in a thing that's called the homeland security system; and when we make these changes, how much difference does it make? We had a lot of discussions in the last couple of days about metrics, and I'm a strong proponent of metrics, because if we can't convince you or the American public that what we have done makes a measurable difference in the security of the country, then why are we doing it? If we can't do it through measurements, then we certainly ought to be able to present a good futuristic argument. We have that

responsibility -- to make sure that we can communicate what we are doing through metrics and why it makes a difference in doing what we're doing.

MS. POULAKIDAS: I would like to reiterate comments my university colleagues made or implied. That is, that the universities of our country really do want to step up and be a part of this homeland security effort and we hope that we have begun to do so to your satisfaction.

There is a threat that our universities are feeling that speaks a bit to General Welch's concern about disrupting some of the fabric of our society: the looming threat of potentially not having as open an academic environment as we have been accustomed to, as has served our country well to date. I'm wondering if the Committee has discussed this and if you have any comments to share.

GENERAL WELCH: No, I don't think we discussed that particular element, but someone may have views.

DR. HAPPER: Maybe I can say something about that. It's a bigger issue than homeland security. The Department of Commerce, Department of State, and Department of Homeland Security can help, but to lay that entire burden on the Department of Homeland Security is too much.

MS. POULAKIDAS: I don't imply that it's a departmental issue, but it is a homeland security at-large issue, something that we've certainly been dealing with a lot more post-September 11.

GENERAL WELCH: Are you talking about visas or classifications?

MS. POULAKIDAS: All sorts of things, visas, classifications, research restrictions.

MR. SMITH: There is one area I'll add to that. There is something which I think DHS has authority investigating, the new category of “sensitive but unclassified” information, and I heard on the radio today that there has been some action. I don't know what sparked it, but it was on the radio as I drove here about “sensitive but unclassified” information and people signing agreements.

So I think that is a concern this Committee should look at -- how that constraint particularly impacts the academic environment and make sure that it doesn't have a negative impact. Universities for a long time have felt that classification should be the primary means by which things are controlled at our universities. That makes it much clearer to us and also is the reason why many universities don't do classified research.

If you start creating gray areas, it creates a tremendously difficult problem for us in an academic environment where you have students who want free flow of information.

MR. VITTO: I do think this issue of “sensitive but unclassified” information is something the Committee should look at. We all can understand the implications and the confusion it is causing.

GENERAL WELCH: The same questions came up relative to DOD; i.e., “basic research,” visa issues, classification issues. Of course, there are laws about applying that to basic research. The law does not restrict applying all those things to applied research, but this issue of “sensitive but unclassified” is causing enormous problems in lots of places, mostly because no one knows how to deal with it. So then when DHS comes forth with a policy for how to deal with it, it causes the angst that you're hearing.

MR. VITTO: My sense is it peaked up immediately post 9/11 and has, I think, had a more rational trajectory towards moving back. I know the Defense Science Board did a study right after 9/11 which ended up getting classified although it was a compendium of unclassified thoughts that in its aggregate was determined to be classified and that was worrisome. I found the classification of the final product a real detriment to distribution.

The Defense Science Board recently completed a similar study where they chose the other approach without any complaint or concern that of violating any sort of compendium of thought process that made something classified. It was more broadly distributed and has gotten better reaction from the various agencies that the recommendations were intended for.

Some classification can in that sense have a stupefying effect, and I can imagine this vague, gray area of “sensitive but unclassified” confusing everyone. This issue appears to be important enough for the S&T advisory committee to at least discuss.

DR. FRANZ: There's a National Academy report issued a year ago now, the Fink Report, which included extensive discussion on “sensitive but unclassified.” But as Mr. Vitto and General Welch have said, it's not as simple as it sounds on the surface.

For example, when we think about the water supply layout for a city, normally we wouldn't have classified something like that in the past, but it becomes sensitive today. And those kinds of things don't necessarily impact academe and basic research significantly.

If you just pare out the parts that impact academe and research, it's a little easier to sort through it and to make arguments for not having such a category. There are other sorts of infrastructure information brought together to point out vulnerabilities, but I recommend that you take a look at the Fink Report for more information.

GENERAL WELCH: The Committee should look into it. One of the difficulties, of course, is there are structures and there are rules for classifying things that are defined and are sacred. There are no rules that apply across departments for “sensitive but unclassified,” so that's something that must be developed if this is to continue.

DR. GAST: I would say that I don't agree that things have been getting better since 9/11, and I think the issues we've had to deal with in contracts and grants to universities have only been getting more difficult. In fact, this Fall the number of these issues was probably at an all-time peak. There was an Association of American Universities Council on Government Relations (AAU COGR) study of 21 universities and the number of contract clauses that universities could not accept due to restrictions on participation or publication of work.

One thing I think the S&T Directorate can do is to be careful in its wording of BAAs and RFPs as well as their contracting mechanisms to ensure that when they are engaging with a university for fundamental research, that they are not imposing the kind of restrictions that they may need to impose on an industry contract that's much more applied.

GENERAL WELCH: Thank you very much.

DR. McQUEARY: I would just like to make a point of stating publicly how much of a pleasure it is to have the quality of people that we have on the Homeland Security Science & Technology Advisory Committee. It's always easy to ask committees to look at what you are doing, that sort of thing, but these people have committed a great deal of uncompensated time. It is a great honor, and I deeply respect and value the inputs that they provide us.

It's in the interest of pushing us in the direction of doing better, and I think their interest and identification of things that we may be already doing something about, by virtue of their saying, "This is something you need to pay closer attention to," spurs us on.

So, I appreciate the work that you are doing on the Department's behalf, members of the Committee, because you do serve a very, very valuable service to us. We greatly appreciate the time and effort you've put into it.

I also greatly appreciate the time and effort of you folks who have come out today to be a part of this because we in Science & Technology have tried to reach out to the community. We're only 250 people and I will tell you, thousands of people who have things to tell us can saturate us very quickly.

We have used the web as our primary mode of communication because we don't have enough people to interact with everybody who would like to come in and talk to us. You should not read that as a lack of interest in what you're doing or have to offer. We are trying to find better ways to communicate because we need your involvement.

I'm speaking from the Science & Technology standpoint, we will not be able to do our job unless we have the full commitment and cooperation of private industry and universities, as well as the national labs. There is a piece of this activity for everybody in those areas to help us do our job.

I hope all of you in the university community know about our Scholars and Fellows Program. We've had a very active program this week; a new group of scholars and fellows are in town. We try to give them exposure to what it's like, but certainly we encourage you to encourage your undergraduate and graduate students to pay close attention to those fellowships and scholarships.

The stipends are reasonably generous, as scholarships and fellowships go, but we need to have those people in positions so that they can have a chance to learn about homeland security and then they can decide for themselves whether that is a field in which they want to enter into upon completion of their study work. Thank you.

GENERAL WELCH: Thank you, Dr. McQueary, staff, committee members, and members of the public for the discussion. This meeting is adjourned.

(The public hearing was adjourned at 11:25 a.m.)

Larry D. Welch
General, USAF (Ret.)
Chairman