Minutes

U.S. DEPARTMENT OF HOMELAND SECURITY

**Homeland Security Science and Technology
Advisory Committee
At
New York, New York**

The Homeland Security Science and Technology Advisory Committee (HSSTAC) met May 20-21, 2004, at various locations throughout New York City.

On May 20, 2004, the Committee members met in closed session and received briefings -- at a Sensitive level -- from Mr. Ed Gabriel, Deputy Commissioner, NY Office of Emergency Management, on details of the New York City's preparedness and countermeasures plans and capabilities. The Committee was later briefed by Dr. Sally Beatrice of the Public Health Lab on their role in homeland security. The Committee then traveled to various operational sites involved with countermeasures.

On May 21, 2004, from 8:15 a.m. – 11:45 a.m., HSSTAC members were briefed at the Environmental Measurements Laboratory – at the classified (SECRET) level – by the Directors of the Chemical & Biological Countermeasures Portfolio, Radiation & Nuclear Countermeasures Portfolio and the S&T Policy Planning. Briefings included: (1) activities and accomplishments of the Chemical & Biological Countermeasures Portfolio, given by Dr. John Vitko, Director, DHS S&T, Chemical & Biological Countermeasures Portfolio; (2) activities and accomplishments of the Radiation & Nuclear Countermeasures Portfolio, given by Dr. Sonya Bowyer, Director, DHS S&T, Radiation & Nuclear Countermeasures Portfolio; (3) activities and accomplishments of the S&T Policy Planning Portfolio, given by Mr. Vayl Oxford, Special Assistant, DHS S&T, S&T Policy Planning. The meeting adjourned at 11:45 a.m., followed by the public session from 12:30 p.m. to 4:00 p.m.

The public session of the meeting on May 21, 2004 in New York City convened at 12:30 p.m. Following is a transcript of the proceedings.

GENERAL WELCH: I welcome you here today and I have a couple opening comments specifically for our guests. In this session visitors are not invited to participate, but only to observe. If you do have input, we'd like to have those inputs, and you can provide those to the e-mail site which is at www.dhs.gov/hsstac.

The minutes of this open session will be posted on the HSSTAC web site. I would now ask Dr. McQueary to give his presentation.

DR. MCQUEARY: Mr. Chairman. Since we've been together for two days, some of this is redundant. Our guests can put into context what we've been talking about. I

want to publicly thank each of you serving on the Homeland Security S&T Advisory Committee. This is a very important committee. While this is only the second time we have met, it is very gratifying to see the progress and level of interest and knowledge that each of you has demonstrated in the two days that we've been together here. So I'm looking forward to your continued advice and support as we go forward in shaping the Department.

I was happy to have a chance yesterday to see some of the operational aspects of what we're trying to do, so we can begin to put into context the magnitude of issues with which that the Department has to deal. What I want to do, very briefly, is to cover some of the important steps that we've taken within the Science & Technology Directorate as a part of the Department of Homeland Security.

To put that in context, I want to remind you of our mission and that mission is to conduct and stimulate research and development and testing and evaluation and to ensure the timely transition of security capabilities to the state, local and operational end users. That's what we're looking for, and we need input from many different sources.

Vayl Oxford talked earlier about the strategic planning cycle; we're pleased with the cycle. The first Science & Technology five-year strategic plan will lay out (we're not quite finished yet) the full R&D test and evaluation program that we have to execute on behalf of the Department of Homeland Security.

We execute our programs in a highly matrixed fashion, and specifically we have four units that constitute the Department. Within the Science & Technology Directorate, we have the Office of Plans, Programs and Budget, the Office of Research and Development, the Homeland Security Advanced Research Projects Agency, and finally we have the Systems Engineering and Development Office. We have the portfolio managers to manage the mission and scientific areas in which we operate. Each of the portfolio managers actually handles work that is done in each of the line organizations that I've mentioned earlier. Quite frankly, it is extremely important that we operate this S&T Directorate as a matrix organization in order to insure deployment of information throughout the various elements that make it up. We will continue to refine the strategic plan; this is just a first step. Strategic planning is something that continues on a yearly basis, but having a firm five-year strategic plan puts us in a much stronger position to evolve that plan on a yearly basis as we go forward. Each one of the portfolios I mentioned will have its own input into that particular plan.

Secretary Ridge testified a couple days ago before the 9/11 Commission and mentioned several things. One that I wanted to touch on in detail because of its importance was the announcement that we are going to form a new Office of Interoperability Capability, and I'll try to be precise what we mean by that.

By the way, the new office will be managed by the Science & Technology Director, specifically. We have not named the individual who will lead that yet. A very important part of the subset of that Interoperability Capability group is a program called

SAFECOM, which we picked up responsibility a few months ago. SAFECOM is an acronym for the name for a program that deals with interoperable wire communications for state and local governments. This is a very large program amplified in detail because of the difficulties we had on 9/11 which the fireman could not communicate with the police and so forth. We're approaching this interoperable communications issue from two standpoints: (1) a near-term solution, which we are working on; and (2) the long-term issue of having the country as a whole have interoperable communications among the various elements that make up the first respondent community. It is a complex problem because a solution cannot be to go in and tell them to throw away what they've got and start all over. The embedded costs of the capital equipment that the community has right now is measured in billions of dollars and, therefore, it is not feasible to say let's start over. So we have to have a plan that will evolve those communications into a fully interoperable capability.

The first step will be, and we expect to have some test sites available not later than the end of September of this year, to put in place interoperable communications that will be constructed at sites where an incident may have occurred or has occurred. There are several companies that have developed what I'll call a communications device that permits radios and essentially any frequency and format to communicate with one another, so this will be the first step that we plan to take in a number of geographic areas in the United States. It will be a first step in moving towards fully operable systems.

We recently issued a statement of requirements, in other words, what are we looking for in the area of the interoperable communications coming under SAFECOM. The point that we touched upon earlier is that this statement of requirements is put together by bringing together people, representatives from some 44,000 different tribal, state, and local entities to have input in this. So we believe that we've touched every single agency or association that has strong interest in making sure that their interests are represented. In some regards we reached agreement among all of these groups that we interacted with that issued that device, so we view this as a first step. I encourage you to watch what happens because it will be the first time that this country has, I think, taken a significant step in the direction of achieving interoperable communications.

Another major step that has been extremely important to us is the creation of the University Centers of Excellence. For the Department of Homeland Security to be successful, and particularly for Science & Technology to be successful, we must have a strong relationship with the university communities and private industry, as well as the federal and National Labs. A way to facilitate that relationship with the universities was to establish the Centers of Excellence.

The first center was chosen in November of last year to be the University of Southern California, and their focus is on the economic consequences of terrorist threats and attacks. And so we felt that was the important first step to look at. We just named, about two weeks ago, two other Centers of Excellence: One is the University of

Minnesota, which is really a consortium of several universities, and their focus will be on post-harvest food supply safety; and the Texas A&M University, which also represents a consortium of universities, and they will focus their energies on the consequences of foreign animal and zoonotic diseases, those that can be transmitted from animals to human beings. We're pleased to have those three Centers of Excellence in operation.

We already have our universities program group working on developing the request for proposals for the next round of University Centers of Excellence. We can afford within our current budgets (current being defined as what has been appropriated and what has been proposed by the President for the FY05) a total of five University Centers of Excellence, so that's the path that we're currently going down. We're not going public yet with what the next two will be, but certainly I can tell you that the examination of the psychology of terrorism is high on the list of considerations as we go forward.

The associated work is in the area of scholars and fellows. The Department was formed in March 2003. We made an early decision that we were going to very quickly establish scholarships and fellowships that will be associated with Department of Homeland Security. We have 100 of those, 50 scholarships for undergraduate students and 50 for graduate students, which are fellowships. They are quite generous scholarships and fellowships. The undergraduate scholarships pay $1,000 plus tuition and required fees for the particular university where they want to go. The graduate fellowships are $2,300 a month, plus tuition and required fees; and the third element of the program is that we expect each one of the recipients to participate for about eight to ten weeks at some locations -- could be Secret Service, part of Science and Technology, or a National Lab -- that way we insure that they have an experience that can be relevant to the development of a strong scholastic base for Department of Homeland Security.

We expect, within the next few months, to announce the next 100, which will bring us to about 20 people that we will have on scholarships and fellowships. Again, we view that as extremely important.

On a separate subject, I'll talk briefly about the Homeland Security Advanced Research Projects Agency. That organization was created by the legislation that formed the Department of Homeland Security. Its primary function is to interface with the public-private sector, if you will, and to do so we've issued six broad agency announcements so far. We have three more that will be coming up very shortly.

The solicitations deal with the standard threat scenarios that we deal with: biological, radiological and nuclear, and advanced security devices. So far we have 131 contracts and we're working hard to get the money that we have appropriated on the streets so that we can begin working on those issues expeditiously. Within a very few weeks, we'll have a broad agency announcement which will solicit research and new approaches for railroad and suicide bomb detection and interdiction.

Lastly, I think it's important to wrap up with a couple comments about where we are here in New York City. It's been over two years since 9/11 in which the Twin Towers collapsed. If you have forgotten about that, go out in the hall and look at the picture of the savage attack that occurred in this city. General Welch made comments in an earlier session when we were discussing these issues about how New York City has really recovered, and to a large measure some of that recovery is that in this past year profits on Wall Street have reached almost $17 billion, that's the highest since the year before 2002 when the profits that year were some $21 billion. Unemployment in the city has gone below eight percent for the first time since 2002. In the first quarter of this year, the city gained some 20,000 new jobs; and the city's spending was about $3 billion in the previous two years. An important statistic is our prime interest rate is down from three years ago. These are all statistics that came out of the NYC Mayor's office, but they are indicative, I think, of the resolve that people in this country have when something happens and what we can do to come back.

While we can certainly mourn, think about, and plan for future attacks, the resiliency this country has is what the Department of Homeland Security is really about and is helping protect. The issue is not about protecting you or me, but it's about protecting this country so that people who come after us have the opportunity to live in a free and open society that we all grew up with. That's fundamentally the responsibility of the Department of Homeland Security in concert with many other government, state and local agencies. Quite frankly, we will never reach the point where we have perfect security. One can postulate a threat that we haven't thought of, but I am confident that the way this country and the people are pulling together to work is very important. We can make ourselves much safer so that we can get to the stage, I believe, which is really the important one.

We need to be able to live our lives so that we can feel comfortable with where we are in homeland security and the way we think about it. Much the same way it is with policemen, firemen -- we don't have perfect police protection or fire protection, but we have enough so we feel comfortable about going and living our lives. Thank you very much for what you're doing to help us on this. I gratefully appreciate it. I'm sure Secretary Ridge could be more eloquent if he were here, but we appreciate people like you who are spending your time to try to help us make sure that we're doing the things that are necessary in order to make this country a safer place for all of us. Thank you.

GENERAL WELCH: Thank you.

DR. SHINE: Mr. Chairman, I think the comments with regard to resiliency is also reflected in the spirit and the attitudes of the personnel with whom we met yesterday as we went to the various places around the city, and I want to communicate from the committee our appreciation to those groups with whom we met, thank them for their willingness to share their experiences, commend them on their commitment and acknowledge the fact that they are operating in the spirit of post 9/11 in an exemplary manner.

DR. MCQUEARY: One of those policemen told me he lost 32 friends.

DR. SHINE: I would like to formally make such a statement, Mr. Chairman, which we should communicate to those folks because they were really terrific.

GENERAL WELCH: One of the comments that I heard after our experience yesterday was about the professionalism of everybody that we encountered. Also, the fact that while we're not yet happy with the capabilities they have, that they are absolutely doing the utmost with those capabilities. I'd like to ask you, Chuck [McQueary], to comment on the overall complexity and how we think about dealing with that, if we have the federal, state, and possibly Department of Agriculture, Department of Energy and the Department of Defense in the equation. We have started to put that kind of a matrix together and to stress the importance of the matrix, but it is a much bigger, broader, more complex matrix than S&T.

DR. MCQUEARY: Although on a minuscule scale compared to the one applied here, any work on the matrix organization reflects the importance of having a clear line of authority and responsibility. If there are not clear lines of communication, conflict between agencies can arise in regards to their individual missions and how they are to interact. So far we have had 10 Homeland Security directives that have attempted, some in detail, to identify what those roles and responsibilities are; and I think that's a major step in helping clarify who's doing what in time of a crisis. Whether or not it's finished, I think the working groups that we put together to engage the various agencies that have a major stake in this form an important relationship. Again, the clear lines of responsibility have to be defined so someone can deal with any consequence.

DR. HAPPER: Chuck [McQueary], I would guess, some of our allies such as the British are trying to do much the same as you are. Do you have counterparts?

DR. MCQUEARY: In fact, I have had several important interactions. Professor David King is chief scientific advisor to the British Government. We have a number of UK people here, and we have learned things from them. We have people heading the national programs who were in the UK about two weeks ago. Again, we want to ensure that we have a good understanding of their capabilities because that relationship is important. Similarly, the relationship with the Canadians is important; Mexico is another issue. But one thing I can comment upon, we have encouraged Texas A&M to bring in a Mexican university as part of the work we're doing on large animal disease because of the important relationship. We also encouraged the University of Minnesota to bring in someone from a Canadian university so we can begin those ties. We talked a bit about the consequences of biological attack, and I'll always remember the first time that was discussed. David King told me the following story:

The British had procedures in place if they had a biological attack, but he said the consequence of having to go public and saying they had cause to wait longer just to be sure, although a few days, was that they had to slaughter twice as many animals than necessary. They reacted instantly with the plans they had in place at the time when

they first made the detections, and that gets to the heart of something we talked about this morning; that is, how important it is in a biological threat to be able to decide early on so you can get on with your consequence management process -- it is very, very important.

Just to follow up. We've also had a number of interactions with the Israelis (they have more experience than anybody, particularly with those who blow themselves up) and with the Japanese, although more limited in that area; and we are beginning to reach out to Australia. We had interactions with Australia just a short time ago. So it is important we reach out, but we, frankly, focus on more things that we need to here. That's an area where any advice and relationships you have and want to follow up on would certainly be pleased to have that opportunity to so.

MR. VITTO: You talked about SAFECOM and interoperability. Is there any encryption associated with that?

DR. MCQUEARY: No, not at this stage, although that will be something that has to essentially be included in it. I'm confident that will evolve. It makes the problem harder as you and I obviously know.

GENERAL WELCH: One of the subjects that comes up repeatedly in discussions with local or state authorities is having enough confidence in the indicators that are present to commit resources and take action, but which may turn out to have been unnecessary. So I think one of the real issues that we need to address is how do you gain that kind of interaction with state and local authorities so that they can indeed take maximum advantage of what DHS can provide.

DR. MCQUEARY: Well, certainly training programs are important. The emergency room preparedness issue response organization has a lot of interaction in that relationship. Our interaction, S&T's interactions with state and local authorities has largely been confined, although we've had a number of interactions on the biological side. For SAFECOM, I mentioned earlier, we didn't bring in 4,000 people, but we brought in representatives from all the agencies to engage in what we're doing. We have an active program within the Department in which we actually issued 12 standards in less than a year, which is quite remarkable compared to the time it takes to get those standards out. To create these standards and maximize their saliency, a standards group was created to gain a consensus from various agencies and localities to discuss the issues at hand. We also work very closely with the National Institute of Standards and Technology, which is under the Department of Commerce, in helping us decide what to do, because they are the experts on the standards issue, and they've been very helpful to us. In fact, they loaned us people, one person in particular, to define our effort in creating standards, and they worked with us to issue standards quickly, which is faster than what they've normally done, and I think that is indicative of their intent.

Back to the point that you really asked about. I've described activities. I did not describe a plan. We have a way to go to plan how to move forward in all the areas where we have responsibilities.

MR. IBARRA: General Welch, one of the things that I see happening in regards to SAFECOM and first responders is that the technology is already out there. There are companies that can already do the interoperability with all the first responders throughout the country. I think you hit right on it, Secretary McQueary, that where we need to get involved is with the local authorities or their organizations, to bring them in, make them feel part of DHS. I do get a sense also that when the federal government comes into a state, the first responders are made to feel part of the group which will open it up much more quickly.

DR. MCQUEARY: I think a point that Secretary Ridge likes to make when he is talking about Homeland Security is that it is not a federal issue, it's a national issue, and our job is to try to muster the national resources on this, not view it as the federal government is going to tell people this is what you're going to do. It will not work. The individual localities, small town, large town, whatever, have to rely on their experience and what they do. We can provide a lot of help and guide them in a distribution that can be beneficial and also help them move in the direction of having a better interoperability capability than what we do right now.

MR. IBARRA: Is there a budget allotted for going out to cities that are over a million-and-a-half?

DR. MCQUEARY: I don't know if we have it broken down that way. Let me describe to you what our intent is. We have within the Office of Domestic Preparedness a grant program. In fact, we already have in place specific guidance that says if you're going to buy communications equipment of this type, here is the standard to which you should be buying your equipment, or you're not authorized to spend government money for that, and we believe that will be helpful in doing that. This is because the groups help to put together the standards themselves, doing what they agreed was a good idea to do. And then we'll be providing government money that will help accomplish that. That's very likely the approach that we'll be using for this, putting together these pilot stations to prove, not only to ourselves but also the country, that what I described earlier, how do we meet and use these boxes that can permit mobile phones and radios to communicate. How we show that it is a viable solution is a first step. We don't want to go out and buy thousands of them and find out there's something we didn't think about. We are trying to put pilot programs in place quickly so we can begin to gather the information to determine how broad based an issue is in the country.

DR. FISCHHOFF: It's one of the challenges and great opportunities that DHS has in its charter; that is, to provide the systems engineering or analysis for the entire operation, even if some are not within its jurisdiction to operate. I would like to see us find some way to discuss how to treat that as science and technology and not just as a management issue, recognizing there are limits, sort of the best practices that are out

there. Vince Vitto had some suggestions earlier that I would like to see us pursuing, systems dynamic or other analytical techniques. It's worthwhile bringing in the people from Health and Human Services who are working a piece of the puzzle to see what interfaces. I think it would be interesting also to bring in some of the British. They speak the same language. They have a very different model in the contingency secretariat. You can go to their web site at www.ukresilience.info/home.htm, and that has its own history. Sometimes it's useful to view one's own model by looking at somebody else's model. .

DR. MCQUEARY: I certainly share your point of view about the system engineering and how it can guide the Department in how we go. We talked about this in a side bar conversation earlier and I think it's pretty straightforward to define the capabilities we have right now because it is what it is. I think it's relatively straightforward to be able to define where we need to get to, although there's going to be a lot of debate about where it is the country needs to get to, and how we want to get there. Part of the problem is how we make the transition, because it fundamentally has to be done. People use the old cliche of changing the engine on a plane when you're flying. I like that analogy, but the solution is not to throw away what we've got and start over. It's got to be how do we evolve from where we are and where we need to get to, and that requires some very carefully thought-out systems work in order to be able to define how you do that. The idea is not to change it over time, but how you make the changes that make the greatest impact to what we're trying to do first and then change the things that are less consequential as we can get to them.

DR. HAPPER: I was very interested in your comments on interoperability. Department of Defense, different services, different parts of the same service -- they have struggled with this as long as I can remember. They're currently going to decide whether to build a new radio called JTRS (Joint Tactical Radio System), and so the question is whether you try to get as much, help as possible from them, because they have faced such similar problems.

NEXT TO MR. OXFORD: We have not gone out with any request to purchase radios or communications devices at all, as far as I know yet. I'd say at this point, it's very clear that some kind of a software defined radio or communications device is how to solve this problem; but in terms of specifications on what those should be, I think we need to put together the standards, and private industry will then try to solve the technical problems because there's a business opportunity there. I think we need to hold fast to the idea of what the standards are going to do, and that's what we're going to do -- listen to the inputs and not be persuaded by who's got what on the street right now. We need to get to competitive forces and let the country evolve in a meaningful way. DOD has a slightly different problem vis-a-vis multi-level security.

DR. MCQUEARY: You're absolutely right.

MR. VITTO: If you can, avoid that. I would hope you can avoid that. That was sort of the heart of my comment -- there's a way to do encryption.

GENERAL WELCH: You mentioned standards. There's another kind of standard, and that is a consequence management standard. We all understand that the actual harm to the public involves more than just what happens, it involves whether or not you can meet the public's expectations. So the question is: who's addressing the standards for cleanup, for example, and who's addressing the standards for consequence management? There was a standard to clean up the Hart Senate Office Building so there would be no anthrax there, so in many cases the only standard we have is zero. There must be no toxin present in order for us to declare that it's an acceptable standard.

DR. MCQUEARY: Which means we couldn't go on the Chisholm Trail.

GENERAL WELCH: Right, I couldn't have lived most of my youth, but in any case, who's addressing that? John [Vitko], do you think you can?

DR. VITKO: Yes, there are two things. Recently issued Homeland Security Presidential Directive 10 established the standards, protocols in all the issues related to decontamination and has responsibility for protection. DHS is the lead in biodefense.

Also, in the biodefense area, we agreed that DHS should have clear delineation of responsibilities. The HSPD initiated a study with the National Academies to provide guidelines on how to clean up contamination and make it safe. They will look at a series of risks that are encountered at different levels of contamination, and following that, there's a policy decision that needs to be made that says what levels we will accept. So we've got those efforts and other things.   HSPD-10 for biodefense gave very clear responsibility, and those words "standards" are in there explicitly and that's important.

GENERAL WELCH: So is there an interface now between those who are doing that and those who know what's possible?

DR. VITKO: Absolutely.

MR. OXFORD: As part of the task, EPA was in the lead due to cooperation with DHS, etc.

There's an unclassified version of HSPD-10 called "Biodefense in the 21st Century" that was issued within the past month, and includes some wording on decontamination at the level of the assignment of agency responsibility, and it specified what's involved at the top level.

GENERAL WELCH: Would you say something about the search for good ideas, the search for applicable technologies, since we're addressing the set of problems that, in many cases, we've never addressed before? How do you reach out and find new technologies?

DR. MCQUEARY: We haven't had to do too much reaching out. The issue has been can we meet with all the people that have the ideas. When I got into this job, because my knowledge is quite limited and it's a little better now but certainly not complete, I believed that the job was more than setting the R&D standards of what the country needed to do in this period of homeland security. As we got into it a very short number of months, it became clear to me, and I'm sure others serving before me, that this country has many things to offer about addressing the issue of the attacking Homeland Security, so we sort of changed our focus of thinking about what the science program should be, to how to take advantage of many of the ideas, prototypes, things that are nearly ready to deploy and that the country already has. That permits us to move quickly toward possible solutions and research programs. One of the key things we had responsibility for is in the Homeland Security Advanced Research Projects Agency, so we have to demonstrate that the process we're using actually brings in non-traditional bidders into what we're doing.

And the last time I had an input that was measured in tens of companies that were nontraditional DOD bidders, we were feeling pretty good about the idea of the approach we're using to bring in people that have not historically been bidding on DOD programs. So I think that's a very positive result. But the reach-out to private industry really comes through responses to BAA's and when people send us unsolicited proposals; we have a process in place for people to go through these proposals, evaluate them, and either decide there's something of merit, or get back to the people that submitted it and tell them no.

I've received some interesting proposals that were easy to say no to, and without saying too much, one that came to me was the idea of putting swords in various strategic places on an airplane so that should there be any terrorists on board, the pilot could release these swords to trusted people that begin to defend the people on the plane. We did not spend any money on that. I mean people are thinking creatively.

MR. VITTO: Do you answer everyone?

DR. MCQUEARY: We try to answer everyone, and I believe we've done a good job, although when we were in the startup phase we really didn't have a tracking system that was very good, so we may have had some that fell through the cracks. If you have somebody that comes to you and says they never received a response, tell them to come back.

MR. VITTO: No, no, it's just a hard thing to do. It can be overwhelming, but it's critically important to stimulate the environment.

DR. VITKO: Even if you're not interested.

MR. VITTO: The worst thing to do is tell them it fell into a dead hole.

DR. MCQUEARY: We get a lot of input. We get Congressional members that have members in their districts that have ideas. I give high marks to most of the Congressional members; they do not simply send us everything that comes across their desks. They try to do some screening.

We've asked in every case that they screen them a bit because we don't have enough people to look into every single idea that comes in. In general, they've done a pretty good job with those things that look like they might have some scientific feasibility, although I wouldn't say it was a 100 percent success, because I did get the one on the swords.

One idea that came through was to put a digital shield around critical areas so that if a plane were to try to penetrate that defined area, you have a way of taking over the controls of the aircraft and precluding them from going there. We also had one come in that said if there was a terrorist attack on board a plane, the pilot pushes a button on a black box and the black box takes over absolute control of the plane and doesn't release until the plane lands. I tried that on a couple pilots and the answer was: Why don't you just let it take off too -- you don't need us. I try not to dismiss any of these things. You never know when a piece of this one or piece of that one might have an idea.

In fact, I began to think that I might be able to do something with the digital shield. Eventually it could be meaningful as it was proposed.

DR. GAST: It seems like one of the challenges with bringing in ideas is that the tendency is always to be fighting the last war. The ideas are generated by public interest and fear based on perceived threats. So the more difficult idea generation is the risk assessment and evaluation of scenarios and future scenarios, and how to weigh all those risks that we've been talking about.

I'm wondering what the mechanisms are for that kind of brainstorming, which is really beyond the things we're working on and aware of and trying our best to defend against to push out towards the future.

DR. MCQUEARY: I believe the answer to that is in good strong systems modeling in which you can do studies, because very often you can do point solutions and the circumstance as we ascribed here, we can fix that problem, but that's not the issue. It's what happens when the problem gets perturbed from that location. You have to have confidence in what we do and cope with variations that may not have been perceived. The way you do that is by having good models that you can use to evaluate what those changes are. As we talked about earlier, we're not there yet with the systems model, but that is a very high, and what I think is an important issue for us to get on with quickly.

DR. SHINE: In regards to that, shortly after 9/11, when the National Academies' Committee was being formulated, there was a discussion about whether, in fact, one

ought to create a group of unusual people, people with criminal backgrounds, people with strange backgrounds, to brainstorm the whole notion of what kind of crazy things, you would want to come up with. As you can imagine, there is some obvious risk with this approach.

MR. VITTO: You did talk about your next University Center of Excellence. At this time there's been a lot of scholarly work. There are some books out now, Terror Networks and a few others, where there was real data, real analysis. You could combine that kind of scholarly work with some brainstorming, and I think you can start doing more of this threat modeling, which you can then get together and do some systems analysis.

GENERAL WELCH: Well, Vayl [Oxford] talked this morning about the threat vulnerability and threat analysis group, a small group of people whose responsibility is to figure out what to do, not with criminals and people of that sort, but rather with people who could look at how you probe the system in order to do that. An important part of what we do, because you really need to have confidence in what you're doing, has a high probability of being able to deter an attack on whatever it is.

DR. BESSETTE: Have you mentioned the work that might be going on in the area of cyber security and cyber terrorism programs?

DR. MCQUEARY: We have a couple small programs in place. I think there is $18 million in the budget this year. One thing we have going on from an S&T standpoint is a joint program at University of California, Berkeley. They're putting together a network that could be used to probe it and measure things that could be done in order to make it less vulnerable. It is a joint project of $5 million or so, so it's not a large activity, but that's indicative of the kind of thing we're doing. The National Cyber Security Division under IAIP and reporting to Bob Liscouski, actually has the lead responsibility for DHS's cyber-security activity. He is a customer of Science & Technology that we needed to bring to bear and we looked at him for one of the requirements in that regard. That's not to say we don't try to think about things ourselves with the few people we've got working this area, but he specifically has the lead on behalf of the Department for what the Department is going to do in cyber security.

I think you'll find a lot of this whole issue of cyber security has got to have private industry involved because private industry owns the bulk of things that could be affected by this. I can tell you that I'm unaware of any interest currently of trying to fix this problem through legislation within the Department. It's a complex problem and the idea of writing some law is not the right way to deal with it.

The point of view that I've expressed publicly is that I believe the issue of cyber security vulnerability is for those companies who recognize what they need to do and how to do it. It can become a competitive advantage. This country thrives on competition and being able to do things that other people can't. And this is an area

where all you have to have is one, or two, or three companies that do get it right and they position themselves, we solve the cyber security problems, and you get the investors thinking a bit about it. I have two companies here that both do about the same thing, both financial investment firms, but one has clearly demonstrated the ability to do this job, that's where I'm going to put my money. I could be totally wrong in that. I think we look at more than just do this or do that. It's more how do you stimulate people to do things because of their own self-interest.

MR. FERREN: It strikes me that one of the very hard, long-term problems facing the Department and S&T is understanding the dynamics of complex systems. In particular, such problems include subjects such as emergent, unpredicted and unexpected behaviors: whether a system is public or terrorist's networks; interconnected technical systems; or interoperability dynamics of systems that were never intended to interoperate, such as communications systems. I wonder if you could speak to your vision of the long-term method of how you address that subject, because it's obviously both operationally hard and scientifically hard but also it strikes me quite critical.

DR. MCQUEARY: I think it gets back to the point of the discussion we had earlier with Dr. Shine. It's how you bring people to bear to think about diabolical things that could be done in order to stimulate what we have to determine what the vulnerabilities are. I don't know any other way to do that. It is an important step because we can take steps to drive terrorists in certain directions. I think you can make things a lot safer a lot more protected in one area than perhaps in another, so you might drive in directions such as that.

MR. FERREN: I think it might be interesting beyond innovative thinking to understand some of the fundamental science that may be driving these systems that nobody who has an operational requirement has looked at in a coordinated way before.

DR. MCQUEARY: Excellent point, but I couldn't tell you that we're doing it. I welcome you to continue to stimulate us on those lines.

DR. PAPAY: We've talked about several different areas of S&T over the last two days. We have not talked about critical infrastructure, although you did mention a little bit when you got into cyber security. Could you say just a word or two about the FY05 budget, and FY06 planning for critical infrastructure?

DR. MCQUEARY: There are 14 identified critical infrastructure sectors, including telecommunications systems and national monuments, water supply, food supply, etc. We are beginning to deal with the food supply system.

As John mentioned in terms of food supply, USDA has the lead on that. But we're stimulating things that could be done.

14

MR. OXFORD: DHS has the lead on about eight other things. We coach here, out of S&T, a working group to develop annual S&T financial plans to deal with critical infrastructure. The first version of each sector infrastructure protection plan is due to the Secretary by the end of the May. So we'll certainly see what the individual sectors are saying are the most important things.

GENERAL WELCH: We'll reconvene on the hour. (Whereupon a recess was taken at 1:50 p.m. to 2:00 p.m.)

GENERAL WELCH: At the end of our first meeting, we established four subcommittees, and subsequently made some adjustments with the objective of helping us develop and form the best advice that we can give to DHS. We defined the focus of the membership somewhat since then, but it's clear from our experience from the last two days here that this is, as we gain more and more information and understanding, going to continue to evolve our view of what we need to do to provide our best advice. And so what we want to do today is to have a set of discussions, led by the subcommittee chairs, that will get us to a common understanding of where we are right now, what we need for some subcommittees to address, how we go about structuring ourselves and focusing ourselves beyond what we have done thus far in order to provide the best advice that we can provide to DHS S&T. That's our objective this afternoon.

I have no idea how substantive the work is that's been done to this point in time, and any substance will be greatly appreciated. But our real purpose is to agree that we have the right structure so we can focus on the right things. We will start with the Mission and Operation Subcommittee report; Vince Vitto and Rich Roca are co-chairing that subcommittee.

DR. ROCA: Let me say two things. First of all, there are six of us on this subcommittee, and I would welcome any of the subcommittee members present to contribute at any time in order to amplify or correct what I'm saying.

Number two, I would reiterate that we view ourselves as a working group of this whole committee, not as a separate arm that somehow goes in another direction. So the work that we're doing, we're assuming is going to be brought to this whole committee and then the committee will dispose of it as it finds appropriate.

This vugraph shows the charter, largely taken from the material that was developed for us as we were defining the boundaries of the subcommittees that were established. I'm not going to bother to read the whole thing to you. You've got the preprint in your book.

I think most of the issues that were raised today fall into general areas of: what direction are you going in, why and how do you interface with others, what's the context of the overall problem, are you working on the right part of the overall problem, and so on and so forth.

I don't think this subcommittee is going to focus on "program number four" being run properly, or is it realistic to expect that they're going to have it delivered at such and such a time. Another subcommittee will do that.

We have both the strategy portion or the direction setting, if you will, and also the governance portion. I read this as, for example, when we say management and business processes, I'm thinking of that which is really, really the first order issues of how the charter is being met. I don't think of business processes as looking at how vouchers are being processed within the S&T directorate and determine whether they meet the government regulations or not. That's the membership.

GENERAL WELCH: The last bullet that deserves a little bit of discussion is that of these two organizational issues. One is the interaction and organization within DHS, and the role of DHS S&T versus integration with the operations people, etc.

But the others are much larger organization construct issues. The one that Larry [Papay] brings up is this whole business about the organization to provide operational concepts and operational architectures that will necessarily reach beyond DHS S&T and, in fact, will reach beyond DHS. We need some discussion as to where we're going to address those. Is this the place or should that be addressed in the Resources and Organization Subcommittee?

DR. ROCA: Well, I'll offer a strong end, as least as I'm thinking of it. When you get down to the details of where you get a particular competency of someone who's a nuclear physicist, or the like, it may be that the Resource team is the better one to understand that. But I think when you're looking at an overall organization, the goal is to protect the country as opposed to any particular function as we're doing.

We're trying to discern just how that maps out; where DHS is in this; where the Department of Transportation (DOT) is, the FBI, the local law enforcement agency? How is S&T laying out that entire construct, and if I remember correctly, S&T considers their systems engineering responsibility to cover that entire construct. Absent other direction, I think this subcommittee would feel itself responsible for making sure that the S&T directorate is indeed doing that, looking at it from an end-to-end perspective.

MS. BORRONE: The other aspect that we talked about was in business practices, as we lay out the construct of the relationships, then how are the business practices supporting that structural relationship? So, for example, Rich [Roca] used the Department of Transportation. Do you have your agreements in place for the Department of Transportation, and then who takes on what relationship or what responsibility under that agreement, which is where the Resources Subcommittee discussion should be focused.

DR. ROCA: We do have a chart coming up, three charts from now, that lays out the initial questions we're going to lay out, and I think we can talk around that chart to some of the first things we were looking at.

GENERAL WELCH: Let's wait until we get to it.

DR. ROCCA: Any other questions with regard to this chart?

This is the subcommittee membership. As far as our method of operation, you can read this yourself; I think there are two items I would like to focus on: the methodology we're going to use poses specific questions, and then understanding the answers to those questions provides our evaluation and recommendation -- whatever might be appropriate in that specific issue, in order to keep the Subcommittee focused.

We will take questions that are formally posed to this particular subcommittee, ones that we self-generate as a result of the charter, and obviously ones from the Under Secretary and his staff, even if they go in a direction somewhat different than we might have thought we would have originally.

The second bullet reinforces the fact that we consider ourselves a creature of this organization, and any recommendations we make are really candidate recommendations for the full committee to consider prior to giving it to the Under Secretary.

I have two slides that deal with the questions. We have the first ones we're going to tackle, and the second ones I call "parking lot." Generally, these deal with issues of direction, and the "parking lot" ones deal with the mechanics of how you go about doing things, to first order.

So what are the underlying goals? Where did you get them? How are you going to know that you are successful in those goals or evaluate your particular progress? The second is the whole issue of threats, which, if you will, is a surrogate for setting the agenda of the entire S&T Directorate.

What is the mechanism by which you identify and prioritize the threats, and then the next bullet is kind of the existence proof; specifically, what are the threats you're working on? How did you identify those particular ones, and what was the basis for it?

And then the fourth one deals with the fact that it's an interrelated problem that is being attacked. DOT has thrown up, as an example, other parts of DHS, entities that are not in the federal government at all, but local law enforcement, whatever it might be.

GENERAL WELCH: Let's be fairly specific. An issue that came up repeatedly yesterday had to do with information dissemination -- I guess the way we ask it often of various agencies is what are you going to do with this information? What's more broadly couched is what the operational concepts (CONOPS) are.

So, for example, we have an operational concept that includes biological sensors, that goes all the way to consequence management. I think there is a significant appetite for that in this committee. The issue is how we go about addressing that, and who is going to investigate that issue, not develop it, but provide advice on how to get that done, and also advice on when we think it is done.

DR. ROCA: I think when we were casting these, particularly the first one, that was our intent. I think it is too subtle the way it's phrased. The issue of CONOPS is a major issue, it's pervasive, and it's a driver for much that has to be done. Based on what we learned yesterday, the comments this morning, and your present comments, I think we ought to explicitly add the CONOPS issue to this list.

GENERAL WELCH: Well, let's let Larry [Papay] and Alice [Gast] weigh in here.

DR. PAPAY: At this point on that particular question, I don't have an issue in terms of that subcommittee taking on sort of a -- call it the CONOPS. I think the distinction from the use of the word "organization," "organizational relationship," I'm getting fairly comfortable with what they are looking at, I'll call it the "high-level relationships," and sort of who they should be dealing with and at that level.

I think what we're talking about, with what we do, is how will they use the National Labs, what should be the relationship with the National Labs? So it's a more specific focus-type thing rather than the higher level.

MR. VITTO: We would want to assess the strategic plan from a completeness standpoint -- does it meet the operational requirements, does it have the developments, have you considered the interrelationships, how is that going to get done? I view you all as worrying about having the adequate resources -- are you spending five dollars on a $50 billion problem, etc. Every question I've asked over the last two sessions -- Chuck, you can read behind those bullets -- I mean we're talking about this high-level system, and we would like to deal directly. One of the things that we can do as a subcommittee is to get inside the strategic plan and the strategic planning process. We would want to get with the FFRDC, and understand how they are going to operate and at what level.

Larry pointed out that you can simulate, as we've done in DoD, right down to a level that will make it impossible. How are you really attacking this threat modeling and then the systems modeling? I mean, I think that's built into these.

But we've decided that the first thing we'd start with was threat -- I mean you have a CONOPS on top, then we decided we'd start with threat and then try to propagate that threat and look at the implications of that threat across other interagency relationships; so we're sort of veering ourselves towards the systems group.

DR. MCQUEARY: I will come back and point out again that we don't characterize the threat. S&T does not do that, that's not our charter and we get the

input for what the threat is from the other part of the organization. That's not to say it's just a one directional flow of information, certainly we have knowledgeable people. For example, John and others in the bio area would get involved in a dialogue. Fundamentally, the definition of what the Department's threat is as it evolves will come out of the Information Analysis (IA) group. That's not to say you can't go talk to them. I want to make it clear that when you say how do we identify a threat, it's a very simple answer: we get it from IA.

MR. VITTO: However, you might get an input from this group through the committee that says given that's the threat or that's the identified threat, we suggest you prioritize it in a particular way, stressing analysis. We're not intel people either, but we might find some issues with too much of a saluting to the specified threat.

GENERAL WELCH: None of this conversation is contrary to this thought, but we need to keep in mind that the reason why, as an S&T advisory council, we're interested in this, is that we don't see how you make decisions as to whether or not a prototype is something that you want to expand into a field system, or whether or not you want to expand generation one or wait for generation two, unless you have a CONOPS plan and an operation architecture in which these things fit.

So at the risk of blasphemy, it isn't terribly important whether the CONOPS is right, because it won't be. What's terribly important is that there be a structure within which things can be reasonably evaluated. Otherwise, you simply evaluate the device on the merits of what the device will do, which leads you to optimize the device, and optimizing the device is almost never the best path to optimizing the system.

We've all got a lot of experience at building the world's best air superiority fighters that you can't exploit fully because we didn't develop the system within which you can use those capabilities. So it's not a matter of you can't work on the device until you have a CONOPS that you're really happy with, it's a matter that you need to start iterating pretty early on.

So I think if we have that as our purpose, then we're all pretty much talking about the same thing, but I want to be sure that you're comfortable with that.

DR. MCQUEARY: I'm comfortable.

DR. VITKO: I think General Welch is exactly right. The only caution I would quibble with on this chart specifically is that the term "threat" always has a classical meaning, and if you ask what is the nuclear threat to New York City right now from intel, they're not going to have one, because they have not seen an intel report that says it. If you use "threat" in terms of vulnerabilities, risks, those sorts of things, I feel a lot more comfortable.

MR. VITTO: It's the way we meant it. We're quite experienced with the intel community telling you there's not an identifiable threat, therefore you can't even think about the potential "threats." We'll work on that.

DR. VITKO: If it's going to go down that path, I want to go back to what Ken Shine said that it may be useful to pick out a couple systems or portfolios to look at in some detail, because there's actually been a fair amount of work there. So we'll take a detailed look at the logic path, where the gaps are, what needs to be done, and that would be the most useful.

GENERAL WELCH: It seems pretty clear that the two that leap out at you are the two that we spent yesterday on.

DR. VITKO: I agree. I'm just saying that you should try to get at a number of those questions at the top level today to allow the systematic unfolding.

GENERAL WELCH: We heard pieces of it. We heard lots of pieces of it yesterday, but all of our efforts to get somebody to kind of knit it together a little bit have not been terribly satisfying. However, we didn't expect to get all the information we needed in one meeting.

MR. VITTO: Larry [Welch], if we're going to be successful with this though, I could identify the areas that we were interested in. I think we need a point of contact. It seems to me, it needs to be done somewhere in the PPB organization. I think we are going to be focused on that part of the organization, although I think there's going to be a portion of discussion on the entire strategic plan. Isn't your plan -- I guess this is to either Larry [Welch] or Chuck [McQueary] -- to identify key individuals who will help us? One of the best things an operating committee can do is to get the right information, and if we can explicitly explain the question, and we get answers from the right people, then truly understanding what we're after is always a big challenge. If we're going to do this effectively, it would seem to me there has to be a point of contact within each of the major organizations.

DR. MCQUEARY: I don't have any problem with how you're doing that. To make sure that we're responsive, I'd really like to have you work through the Executive Director and his staff, so he can fan it out and reach into the organization as needed, because in general, the portfolio manager is where you go to get information on each of the programs.

DR. ROCA: What I'm hearing about this chart is the whole issue of CONOPS, and that which surrounds it will be explicitly stated. The word "threat" should be treated with care so it's not misinterpreted. We also ought to understand the degree to which S&T is or is not a free agent in declaring what the threats are and what the priorities are.

GENERAL WELCH: I would almost ask if we don't really mean vulnerabilities.

DR. MCQUEARY: That's a good suggestion.

DR. ROCA: There are the issues that we identified in our first meeting that we put for later consideration on the chart entitled "Questions for Our 'Parking Lot'." Again, you can read them. They tend to be more about how you do business; for example, look at the matrix portfolio managers. I guess my questions are, and they are more to the DHS staff: Are you interested in any of these being explored? Are there others you would rather have explored? Are any of them ones you would rather put off? Are any of them ones you'd rather see done sooner rather than later?

GENERAL WELCH: Just to begin with, I wonder if those are your subcommittee's responsibilities. I would think the first two are Larry's [Papay] committee. I take that back. I wouldn't say I think they are; I'm asking. If Larry [Papay] doesn't think they're his subcommittee, they're not his subcommittee.

DR. GAST: We did talk about resources involving not only the financial resources, but also human resources; so in that sense, understanding whether the human resources are correctly deployed and interacting would be something we would have taken up in that context.

DR. PAPAY: Which gets us to the second one.

DR. GAST: We could look at management and business processes in the context of deployment of human resources.

MR. VITTO: Larry [Welch], the top two came out of the first page [charter] in the sense that we were looking for gaps, not resources and not criticism of the portfolio. Is the matrix structure based on the CONOPS? Based on the vulnerability analysis? Then when you map what you learn from that against the portfolio management, you said it yourself earlier, are there gaps, what about the interfaces? So we saw this as logical, and it's only at that level that we were going into that. I would imagine the same two things could be on your list with a slightly different emphasis.

DR. PAPAY: This gets down to words and the interpretation of words. For example, B [on the chart] says, "the matrixed 'portfolio management' structure." The word "structure" can be interpreted to mean organization. You're looking at it as the matrix -- the structure of the matrix and are their holes and gaps.

MR. VITTO: And have we identified something from the operations concept that is not being covered fully because of the way the stove pipes are laid out or the way the cross matrix is structured?

DR. PAPAY: "Structure" is a word that can mean different things to different people.

GENERAL WELCH: I think we have agreement here.

21

DR. GAST: It does bring up the general issue that there needs to be a lot of interaction between the subcommittees. Programs and Resources Subcommittee obviously goes very well with Mission and Organization Subcommittee, and perhaps we can exchange our work product in between meetings.

GENERAL WELCH: Next up is the Program Subcommittee.

DR. HAPPER: Let me introduce the Program Subcommittee; it consists of Ken Shine, Ron Atlas, David Franz and me. We welcome anyone who would like to join us in any of our meetings. We'll try and keep you informed on what we're doing.

While we're trying to get this high tech equipment working, perhaps I can read you our charter which comes out of the grandfather document for our group. It says, "To evaluate the mission relevance, technical quality, and management of the S&T Directorate's programs; as well as to identify research areas of potential importance to the security of the nation."

We've had one meeting by conference call, most of us participated, and we occasionally see each other informally in other venues. We plan to meet at least once a quarter, either in person or if things are really tight, perhaps by phone.

The deliberations of our subcommittee will be judgments on the excellence and relevance of the programs of overall HSSTAC mission, and how the program efforts are balanced to address the most important vulnerabilities facing the nation. Of course, we'll prepare a regular report for the full committee, so we'll be ready to discuss what we've learned at each quarterly meeting.

Let me tell you some of the issues that I've identified. I'm not sure that our full subcommittee has chomped on these enough to be certified as issues. Number one is we saw a lot of counter-bioterrorism efforts yesterday. My impression is that it's taking a lot of resources from the Homeland Security budget, but it's probably appropriate.

We would like to understand a little better what the balance of investment on countering bioterrorism is with other programs that are also important. For example, we heard about radiation and nuclear threats today. One threat that worries me a great deal is, if you look around at what really kills people, by far the most people have been killed by rather low tech things like ordinary explosives. This very difficult problem is something that I don't understand very well yet within the context of homeland security

The attacks in Madrid were conventional explosives. Our domestic attacks at Oklahoma City were conventional homemade explosives. In Russia, most of the terrorist attacks on Chechnya were with explosives. I think one question is: Is this just an unworkable problem, or is it something that there is a chance of doing something with fresh ideas, and that homeland security could thrive. I don't see another agency

that is more likely to have that as their central mission than the Department of Homeland Security.

DR. MCQUEARY: And we agree with you completely.

DR. HAPPER: I'm glad to hear that. I realize it's hard to get the whole program out right away.

I want to talk a little bit about nuclear weapons. We heard this morning about how difficult it is to handle special nuclear materials.

GENERAL WELCH: I remind everyone that we are convened in unclassified, open session.

DR. HAPPER: The real defense is off our shores, and we are hoping that the programs in the Department of Homeland Security work together with the Department of Energy (DOE) and with the State Department to address the sources of special nuclear material, and the big source is Russia. We hope that, Chuck [McQueary], you and Secretary Ridge will push this foreign interception as hard as you can. This is very much on my own mind personally because I spent a week last Fall in Russia looking at their highly enriched uranium and plutonium. Most of the defense around these facilities is being paid for by the United States to hire guards, to put up fences, to have portal monitors. And I don't know how long the U.S. can be expected to do that, and at some point, you have to count on the Russians to do the job themselves. There are a myriad of issues that need to be addressed.

Here is a list of special issues ["Special Issues" chart]. This is a long winded way of saying that where DHS has to rely on other agencies, they should not be shy about insisting that other agencies contribute to their charge It would help the Nation a lot if people all over the world would find it repulsive to put a nuclear weapon on New York or on Washington and if they could somehow prevent that. Even though they don't like the U.S. very much, they might say this has gone a step too far, this should not happen. The sort of thing I'm thinking about is this new satellite broadcasting system for Arab News. I don't know who supports that, but it's supposed to give a better view of the U.S. and what it really stands for than what you see on Aljazeera. Perhaps there may be ways to have exchanges of people with the Muslim world and the United States to build ties. We did that during the entire length of the Cold War, and in the end it paid very helpful dividends. We built up a collection of people who were certainly not traitors to the Soviet Union, but they helped calm down some of the worst excess that existed there.

MR. VITTO: This is a critically important issue, and there are DOD, Department of State, and a whole variety of others including the Council of Foreign Relations (who has 15 independent studies going) very aggressively looking at this issue. There are a lot of studies going on concerning that topic in the entire interagency arena, and I'm

involved with one right now. So I just don't know that it's something we, or your group, needs to focus on.

GENERAL WELCH: Or to continue that conversation, just off the top of my head. Number two [on the "Special Issues" chart] is probably DHS business. Number three is definitely DOE business. DOE has all the funding to do that, but the Defense Threat Reduction Agency (DTRA) is assigned to DoD. Number four is not DHS' business.

DR. HAPPER: You say number three is not DHS business, but the part of that business that DHS has is almost impossible. The very last stages of getting HEU to cross our borders into the United States is a terrible job to have compared to keeping it in place. For DHS to be responsible for this supremely important thing at the very last stages when it's almost too late is terrible, and DHS should have full support. I mentioned to Chuck [McQueary] the way to get that support is to get the Russians to take it more seriously, and the way to do that is to constantly lean on people like President Putin when they have the Sea Island [G-8] meeting, which will take place soon. President Bush will have talking points, and one of the talking points should be: you should pay closer attention to special nuclear materials in Russia. If you get that message from the U.S. and from our allies, eventually I think it will help us, at least as much as putting a few more portal detectors at our ports of entry.

GENERAL WELCH: My issue is not whether or not it's terribly important, not whether or not somebody needs to confront President Putin with this, it is that it's DOE and DTRA's responsibility to do that. They're clearly assigned that responsibility. It's not a gap. We may not be happy with how it's done, but it's clearly assigned and it's not a gap.

DR. MCQUEARY: In conversation we had, I simply took your input as being one that we ought to come at this in multiple ways and try to move it forward, so I don't feel uneasy about our taking a good idea and then depending on present discussions taking the lead. General Welch is obviously right.

DR. VITKO: Without talking details, this is working very high policy issues across the Homeland Security Council and the National Security Council with the interagency present.

DR. FISCHHOFF: A question of form rather than substance on this. During the Cold War the nature of our R&D effort and how it related to our relations with other countries was an important issue that came up in places that are classified and jointly work together. Over the longer term, it strikes me that that might be an appropriate topic for the S&T Directorate. I think some of these things reflect policy issues that are outside of our brief. On the other hand, there are things that may be possible from knowing the details of the technology that might seem otherwise impossible, that you can collaborate if you know the details of it. And we might be able to shape some of those relationships that might be within the realm of the Operations Subcommittee.

DR. ROCA: These I would characterize as issues of whether programs exist to do so, as opposed to whether programs are going to deliver what you expect them to deliver, given that they exist. Is it important to your Directorate, Chuck [McQueary], to have this body speak to what confidence we have in particular programs and whether we think they're going to deliver, when you think they're going to deliver, roughly what you think they're going to deliver?

DR. MCQUEARY: Probably -- the answer probably depends; but, in general, I would say yes.

DR. ROCA: If that were so, I would think you would want a bullet on here that would say that.

GENERAL WELCH: This is "special issues" [slide entitled "Special Issues"]. I presume there are other issues?

DR. HAPPER: We really have not gotten started yet. These are initial issues.

GENERAL WELCH: How do you plan, just in general, to get through the technology program? You plan to do a sampling?

DR. HAPPER: Well, for a start we're going to look at the budget and see where the money is being spent on programs so that we know how the resources are allocated now. Then we're going to put our finger on the biggest effort as measured by dollars in trying to decide if this is being done properly, as best we know, if it is duplicative of other efforts and other federal agencies.

DR. ATLAS: For better or worse, this subcommittee is populated with biologists, and I thought that might be reflective of some of the large investments that the Department has decided to make in BIOWATCH and in the center that will be constructed maybe at Fort Detrick, the National Biodefense Analysis & Countermeasures Center. I think it would be wise certainly for us to look at those two programs and give you advice on the adequacy, or are they too large? I mean where are those relative to your investments? I'm sure that we will be moving down, and I suspect we're going to need additional expertise from the parent committee as we deal with some other areas, at least as I sit through the large briefing areas that I am interested in but not competent in.

Beyond that, I would hope at some point we would look at some other documents, either the Presidential Directive to see where the Department is supposed to be relative to their organization, make sure the programs are meeting those mandates or even go back to the original National Academy report, Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, and look at the major recommendations, things like having a national testing bureau for the products involved in defense efforts and ask whether or not the program on standards is actually

covering that full mandate that the Academy virtually charged the nation with moving forward. So those have some of the more central topics that I'd like to see us tackle. I suspect that's going to mean we have to come to Washington as a sub-committee at some point and meet with some people who can show us some documents and gather the program managers to help us understand the details of the programs.

GENERAL WELCH: So, in general, you're going to start looking at the large technology programs? It's not exactly sampling; but of this very long list of technology programs, do you have in mind some approach to the longer list? Are you just going to look at the top group, or are you going to pick from the list?

DR. HAPPER: We're going to weight them by where we judge the emphasis goes, and then we're going to look at those that are not emphasized very much and convince ourselves that the lack of emphasis is justified, that they're not deserving of more support. The best way to do that, of course, is to look at a budget, and if the line items are clearly identified, we will probe into those programs, find out who controls them and what's being done or what's planned to be done.

GENERAL WELCH: Anything else? Any comment? Chuck [McQueary]?

DR. MCQUEARY: No, having looked at the programs, I think it would be a helpful adjunct until we are in a better position to use a solid system approach and to characterize what the investment should be. A lot of this was based upon the considered judgments of very capable people, and so it has the element of human estimates, but we welcome the examination by your group, and any thoughts you might have.

GENERAL WELCH: The Resources and Organization report?

DR. PAPAY: The Resources and Organization Subcommittee met on May 3. We had two objectives at the meeting: First, to get our charter and statement worked out; and secondly, to take on our first assignment, which deals with the relationship between the S&T Directorate and National Labs.

Our charter is to evaluate whether financial and human resources, policies governing them and the laboratory infrastructure are adequate to meet the goals of the Science & Technology Directorate, etc. We are a lean, mean group, only three members on our subcommittee, so we can actually hold a meeting with two people, and still have a quorum.

At our first meeting, a group joined us because we had a special issue come up, which I'll get into, and we thank them for joining us. Bran [Ferren] was going to meet with us. He couldn't make the schedule and now he's removed himself from our group because we're dealing with the labs and he has a possible conflict.

Our methods of operation are very similar to the other subcommittees; that is, we will hold at least one meeting interspersed with meetings of the full committee doing reviews as appropriate. We plan to look at the adequacy and the proper utilization of the financial and human capital allocated to S&T; thus, the timing of our reviews will be set to meet the Directorate's annual budget cycle.

We need to feed this committee the information that we've taken a look at. The Program Subcommittee will have input into that too, but we need to time our meeting such that when this committee meets you can turn to us, and we can say something to the effect that we've reviewed the budget and find it is adequate or they don't have the right staffing, they don't have enough staffing, things of that sort.

Under the "special issues" chart let me just take a minute and give you some background information, because we're in the process of reviewing the relationship between the Department's Science & Technology Directorate and the National Labs.

It is our current expectation that we will have a draft report forwarded to the full committee for review and discussion at the August meeting. It's a tight schedule. We've got some information coming from the new Homeland Security Institute which would help us. We need to have at least one additional meeting with some of the laboratories, as well as other interested parties, before going forward.

The issue gets down to this. If you look at the enabling legislation that stood up the Department, Section 309 of P.L. 107-296, November 25, 2002, it talks about the use of the National Labs by the S&T Directorate, and it says you can use the labs by joint sponsorship, but it's like two riders on a horse, only one of them can hold the reigns, and the person holding the reigns is the Department of Energy. It talks about direct contracts, but the direct contracts are in there only for work transferred from the Department of Energy to the Department of Homeland Security. Third is a "work for others basis, and the fourth is the usual, other methods as provided by law.

The point here being these are DOE labs. The RFPs are put out and the contracts are let by the Department of Energy. The strategic goals for DHS and the Directorate really speak to awareness that there's a new need to meld the scientific community with the intelligence community, that there are some unique aspects to the programs defined here, and that there is a need for organizational excellence within DHS. It's going to be an enduring program, and needs to have a scientific cadre which meets that. The question is: what's the best mechanism to use to accomplish that.

There are some DHS laboratories, the one that's going to be stood up and Plum Island. There are University Centers of Excellence. There's the new Homeland Security Institute, but there's a mixed bag right now. You don't have to have a single way of doing business, but you don't want to have a complicated way of doing it, if things can be simplified. But let me just say that it's an interesting problem.

There are nine labs (technically eight labs and a Nevada test site) who have indicated that they would like to work with DHS, and although you'd like to work perhaps with all of those entities, I don't think you want to have separate contracts going out to all of those through another body. Enough said on that point.

There are three potential issues listed here ["Special Issues" Chart], and actually I've written in a fourth one based upon a comment that Chuck [McQueary] made this morning: the long-term capitalization requirements within the Directorate from a laboratory point of view.

Also, the second bullet is the one dealing with budget connectivity within Science & Technology and the operating directorates. For this business of going forward as technology moves through the directorate and goes commercial, there needs to be an out-year budgeting mechanism which allows the operating entity within DHS to begin to get a placeholder within the budget for operational deployment. We think that's an important issue, and one that needs to be addressed by the subcommittee.

DR. MCQUEARY: Could I comment on that? Unless Secretary Ridge changes his mind or changes our minds for us, we're going to put the budget wedges in our budget, although that's not the place where long-term should be. It should be in the operational plan and make sure it's covered, and we're going to put a place on it.

DR. PAPAY: We would like to take a look at that. The others are pretty well straightforward in terms of adequacy and proper distribution of resources. And since its going to be a five-year planning horizon, we can take a five-year process. That concludes the report of the subcommittee. Again, when we say resources, as I mentioned earlier, it's operating budget, capital budget, and human resources.

GENERAL WELCH: Can you say a little bit more about the organization issue?

DR. GAST: Well, at least initially our organizational issue has focused on the National Lab question, so in some sense we were the Resources Subcommittee. We became the Resources and Organization Subcommittee, and we're thinking through how to meet that charter.

DR. PAPAY: The other part of that is to look at how from an organizational point of view, the S&T Directorate has set up this pipeline. You've got parties sitting here from the programmatic point of view, and then you've got the other three offices set up for the proper flow through. I think looking at that to make sure we don't have any constrictions in that pipeline, and that the pipeline, in fact, does expand as you go downstream, and the adequacy or the appropriateness of how hand-offs are made.

I don't think we're going to go in and suggest the boxes [in the organization chart] should be rearranged or anything like that. I think the organization is a management decision. But if we see issues arising from the hand off, and I'm not

suggesting that those are going to occur, I think that's the sort of thing we need to look at.

We will also be looking at what should be done perhaps using in-house talent, the laboratories they do have, how we work out this arrangement with the National Laboratories, things of that sort.

GENERAL WELCH: One of the issues that comes up again and again, using BIOWATCH as an example (simply because it's the first thing out here, not because it's inherently difficult), is the hand-off of systems. The experience that most of us have, even though you have an R&D organization or an S&T organization (an operational organization), you have a user who spans the entire spectrum. That is, when you deploy a weapons system, the owner of the weapons system is also the developer of the weapons system, and also owned most of the S&T. So the hand off there is within an organization that maintains birth-to-death (cradle-to-grave) cognizance. And so one of the potential organizational issues that comes out of what we've heard so far, or what we have not heard so far, is how does that birth-to-death attention take place. As an example, BIOWATCH has now been handed off, but obviously BIOWATCH is not finished. There's an enormous amount of S&T that would be continuing, so I guess it's not quite clear to me how that birth-to-death organization actually operates.

DR. MCQUEARY: I think that's an important area because, quite frankly, BIOWATCH is not perfectly clear to us either in a sense of how it's going, as you summarized very well. But it's not so clear to me that I want to have S&T continue to take on responsibility for operational capabilities, because the risk is we become an operational unit as opposed to Science & Technology.

DR ATLAS: On the other hand, you've got second generation technology.

DR. MCQUEARY: And this is the rationalization that I've convinced myself that BIOWATCH is in the embryonic beginning of a capability and provides a very important capability; but as John [Vitko] described, we have a long way to go for this thing to come to what we view as the system that we want to point to, where it needs to be. So on that basis, since it is going to be evolutionary, I can see us operating something that's got pieces of BIOWATCH, pieces of BIOWATCH II, pieces of BIOWATCH III, and evolving this thing to be what we want it to be and scientifically what the right answers need to be.

But if we do that with every single thing (BIOWATCH is going to be roughly ten percent of our total budget), we can soon find ourselves in a situation where the operational aspects dominate the S&T piece, and I don't want that to happen.

DR. PAPAY: I think there are mechanisms for involving the ultimate internal customer, the operating entity within DHS that would be responsible.

DR. MCQUEARY: That's part of the problem too. There isn't an ultimate internal DHS customer.

DR. PAPAY: One of the options may be to invent internal customers within an operating organization.

DR. GAST: I was just going to say that; in addition, we did spend some time talking about the integrated biodefense strategy and the organizational constructs to integrate the medical community and the intelligence community appropriately on both ends -- the intelligence community on one end and the medical community on the other.

So depending on how you interpret our role as the subcommittee, this organizational aspect was something in addition to the interaction with the National Laboratories we were taking very seriously.

GENERAL WELCH: It seems to me that's very much within your charge.

DR. ROCA: I wanted to ask a question given the conversation about the operations part of the Mission and Operations Subcommittee. I had been assuming that operations referred to how S&T operates, its own domain as opposed to the operations in the field of how you did BIOWATCH or whatever. If that were true, then the operations M&O would worry about how to go from one phase of development to another phase, such as testing.

GENERAL WELCH: I guess the intent of operations was operational concepts [CONOPS]. Now, that doesn't mean that's what we still believe.

DR. ROCA: No.

GENERAL WELCH: It's on that level.

DR. ROCA: Okay.

GENERAL WELCH: Not only internal operations.

DR. ROCA: Given that, then I think there would be issues that we have listed in our charter that we're going to e-mail to you.

DR. GAST: No thanks.

DR. PAPAY: I think that's the basis for some of our chairman's questions. You do the "what" and we will do the "how."

DR. ROCA: But how the matrix portfolio structure is working, I think that's an operational issue.

GENERAL WELCH: I'm not quite sure.

DR. GAST: You're operation --

DR. ATLAS: I just want to emphasis what I said before: I see BIOWATCH as something that we have to look at very closely on the program side, not just because of the question of the content, but also for just these reasons -- that it's an example of one in which accession to new technology (the generational development; the question of deployment of that technology; where, when and how far in the context of S&T) overlaps in terms of interests.

DR. PAPAY: That's why I said there needs to be coordination.

GENERAL WELCH: All the subcommittees are intended to overlap.

DR. ATLAS: Sure. But I do think that we have a primary responsibility on the Program Subcommittee side to say this is a major program and to question its goals and objectives, how well they are being met from an S&T point of view, and how does that interact with the way in which deployment takes place. We may have something to contribute with regard to BIOWATCH II and III just as the Operations Subcommittee does.

GENERAL WELCH: Yes. I think the operations and the technology obviously have to be closely interfaced.

DR. FRANZ: I would like to follow on to your point and also Alice's [Gast]. It's my understanding that there is a hand off at some point between NIAID, Tony Fauci's staff, out of the tech base into the preclinical trial pillar.

DR. VITKO: Absolutely not.

DR. FRANZ: So that is gone.

DR. VITKO: There are no responsibilities within DHS.

DR. FRANZ: There was a preclinical trial pillar that was briefed early on.

DR. VITKO: It's not there. That was part of the cleaning up. There is no biomedical.

GENERAL WELCH: So you're not involved in syndromic surveillance.

DR. VITKO: First of all, we were talking about progress of drugs to clinical vaccines.

GENERAL WELCH: Now I'm talking about medical.

DR. VITKO: Let's answer one question, then we'll get to the other one. The answer to that one is clearly a no.

We're not involved in that -- in fact, that whole clinical process goes through there. Our only involvement on the biomedical countermeasures is in the context of Bioshield where our responsibility is to certify a material threat to this country, to estimate the size of what's needed, and to support those size and requirements for the strategic national stockpile. With respect to the question that you raised about biomedical surveillance, we're doing a small amount of work in biomedical surveillance. The President has a bio surveillance initiative. There's an integrated initiative across multiple agencies. There are sector specific responsibilities, so all human health data will be handled through a separate line. There is a responsibility for DHS within that that deals with the integration of multiple surveillance, health, animal food, as well as environmental sources, environmental water sources, air, water and food, and intelligence data. That fusion activity is to occur within DHS and the Information Analysis and Infrastructure Protection (IAIP) Directorate to support a more integrated CONOPS picture that DHS uses for managing an incident of the national response plan and the national incident management system.

GENERAL WELCH: What further complicates this whole question, again not to start with a blank slate, but we have to relate things to our own experience, and that is, in this case, the customer is not the Federal Government, or at least there is a customer that is not the Federal Government. So when you think about how you relate continually in S&T, continuing product improvement, etc., to the fielded product, not only is it not encapsulated within an entity like a military department, it's not even encapsulated within the Federal Government. It seems to me that that raises the complexity of making product improvement, follow-on S&T, fielding, upgrades, etc., that it makes that far more complicated than anything that any of us have dealt with in the Defense Department.

MS. BORRONE: I think the point you're raising, Larry [Welch], though, leads me back to the thought that we started with: risk and assessment of risk, and then how that factors in throughout the cycle of the development of the product for BIOWATCH, for example, particularly given other users, and so I think it leads us back to a question that our subcommittee focused in on immediately, which is we need a better understanding of not what the vulnerabilities and risks are per se, or how they're identified per se, but how we take those and make judgments about the priorities, the level of investment, and then how we see the resulting products actually meeting those expectations or thought to be expectations, and whether they are or aren't, and then whether they justify the additional level of resource depending on the continuing thinking about threats or risks and vulnerabilities. At least that's what your comment sounded like to me as I was listening to what you were talking about in the Resource and Organization Subcommittee area.

DR. PAPAY: I took it a little bit differently. I think looking at it on that level -- whether you call it programmatic or mission, or what have you -- I think what the Chairman was suggesting from the Resource and Organization Subcommittee is how to effectively translate technologies to the field where your customer base is 44,000 entities, and it may be public health entities for technology A, it may be ports and harbors for technology B, and it may be fighters for technology C. I'm taking as the charge here that there may be a single way or multiple ways in which to get technologies out to the user community, and I'll use the phrase in "the best manner possible," without trying to get into it at this point in time, because it may be different approaches for different user communities.

GENERAL WELCH: Yes. If you can do that, we will make progress.

MR. FERREN: I have just one point. This strikes me as being critical to success, but it's also important to note that this is something that the best companies in America do very badly, which is transition from R&D into production and such. So it's not like this is a basic skill set where you just looked to best practices and industry and government. This is a national level problem, and it's one that is very hard to look around and say, here's how you would go do this. I think it's further complicated, in my observations of government, by the acquisition regulations that most agencies work with it, because the ability to react fast and to transfer anything rapidly is contrary to all of the checks and balances that are put in place. I think someone should be looking at this from an acquisition's perspective of how to get the best leverage specifically to address this issue of rapid technology transfer. I think it's doubly hard for government.

DR. MCQUEARY: We actually have special legislation that's included in the Act that created the Department of Homeland Security to be able to do fast contracting. One very important example of the work that we're doing is on Counter MANPADS, the counter to the shoulder-fired missile which is a threat to jet aircrafts. We went from issuance of a Request for Proposal (RFP) to having three contractors under contract in four-and-a-half months. So we're working very hard to use these legislative authorities. Basically this puts us in a position where we don't have to put with up a protest if somebody doesn't like what we've done. We sort of avoided that aspect of it in some cases depending on which one you use, but your point is extremely important. I cannot imagine a scenario where we say we know exactly what to do, it's going to take us seven years to get there. Who would ever listen to that and say this is the government. So you have to have that to be able to react quickly.

I also think it would be helpful if the Committee took a look at the Homeland Security Advanced Research Projects Agency. We're getting pushed back in some particular quarters in the government who think HSARPA should be just like DARPA. If we were to move in that direction, it would force us to create yet another organization reporting to me that deals with the corporate interface by dividing execution responsibilities up differently, so I would appreciate a view. As I stated earlier, my view is we're going to evolve into something that can have more of a DARPA flavor, but we shouldn't start out that way.

GENERAL WELCH: Are you ready to take that on?

DR. PAPAY: That's fine.

GENERAL WELCH: We'll discuss it at the next meeting. The Outreach Subcommittee?

DR. BESSETTE: The good news is we're the last presenter of the day. We had a couple of meetings by phone, a face-to-face meeting, and considerable e-mail exchanges as we prepared our presentation. The Outreach Subcommittee is composed of Baruch Fischhoff, Tony Ibarra, Ernie Mitchell, and me; and we view our mission as part of the legislative mandate for the Department, which was outreach. The Outreach Subcommittee will deal with matters concerning communications with university academic research institutes and commercial facilities.

And so based on that slide which you see and on which we had spent considerable time, we formulated a two point mission statement. If I were to reduce those two bullets into two words, the first word would be "technology," and the second word would be "communications."

The first bullet is the mission of the Outreach Subcommittee which is to augment the Department's efforts in securing skill sets. We chose the term "skill sets" to represent not only products, but also systems approaches, methodology and skills that would be brought to bear from U.S. academic institutions, large and small businesses, and governmental and non-governmental organizations for homeland security.

In that bullet we wanted to reflect the fact that our role was not to be a lobbying group, to be a testing group, or to focus on just products and widgets, but rather to look at the systems approach as to how the Department evaluates those technologies as they're brought into the Department, the methods used, and whether it is securing the best systems that would assist in homeland security.

DR. MCQUEARY: In the part where you're talking about U.S. academic institutions, make sure that it includes Minority Institutions and, specifically, Historically Black Colleges and Universities, because there's strong interest in the colleges and universities being a part of what we're doing in the Department of Homeland Security.

DR. BESSETTE: That's a good point.

The second bullet deals with the efforts to improve communications -- among those groups and the Department of Homeland Security, as well as the public. We thought that was a very important concept, and also took advantage of some of the subcommittee members' expertise in addressing that issue, which we felt is very important -- where the rubber really meets the road. The communications of these skill sets, as well as responses to the public and to the other customers that the Department

might deal with, such as academics, universities, business and governmental laboratories, are very important.

As we indicated there, this effort seeks to improve communications among these groups as well as the public, who are concerned with the impact of their work on homeland security. So these two bullets tried to capture our mission, and I would ask if there are any comments or if any of the other members wanted to add anything to that.

MR. IBARRA: I'd like to just add a couple of items in regards to the government's procurement process that can happen relatively quickly, four months, which is phenomenal.

I think, secondly, we have to look very carefully at the small business sector. Small business is able to ramp up rather quickly compared to large corporations. I liked the analogy that Russ used. It's like looking at a large cargo ship versus a small canoe. That canoe can turn and move quickly. And with small business that's out there, they look at the needs of security that are occurring.

In the security industry, I would say probably five percent of those companies are on that cutting edge of technology and at times they may be on the bleeding edge. That's why we have agencies like the National Labs to assist these companies, Small Business Innovative Research (SBIR), the universities, and to look at this kind of technology that's out there, and then actually put it into either a pilot program or a workable system.

Surveillance is becoming a major part of security today, because visuals are tools that law enforcement can utilize to assess situations. They're a smart technology now.

I see small companies out there that are putting programs together that can look at abnormal behaviors that will create alarm conditions that then require human interventions. There are software programs out there that will look at unattended baggage, somebody drops baggage off it will create an alarm condition. We're going to see a move towards this. I think in order to deploy that rapidly, we again need that procurement arm, but we also want to look at these smart companies that are out there.

DR. MCQUEARY: We do have an SBIR program; we have $20 million set aside this year. We're currently in contract negotiations with 66 small businesses as the first step in the SBIR process. We do have 2 1/2 percent of the Research, Development & Acquisition (RDA) budget set aside for SBIR, so your point is well taken.

DR. BESSETTE: I think our mission would be to look into the Department's activities with those companies and become more informed about them.

DR. GAST: I was just wondering, the second bullet talks about communications with those who are concerned with the impact of their work on homeland security. It

sounds like the focus is on communications within those working on homeland security rather than communications to the outside world who would be interested in the impact of homeland security efforts to protect them. Maybe this is just a wording issue or the tone of the second bullet.

DR. BESSETTE: Because we certainly did not mean internal communications. We meant the external communications, as I said from the beginning.

DR. ROCA: Is this the group that concerns itself with how DHS effectively tells the public that they're in a pickle, or they're not, or whatever?

DR. BESSETTE: That's what we're trying to convey by bullet two.

DR. MCQUEARY: I'd encourage you to interact with Secretary Ridge's Homeland Security Advisory Council (HSAC) as you develop this advice. They also have an interest in advising the Secretary.

DR. FISCHHOFF: The point is that we need science and technology that will inform the executing entities, that's ultimately a political decision.

GENERAL WELCH: I would call that "expectation control." You really need an understanding of the technical and capability issues so that you insure that the public has realistic expectations.

DR. FISCHHOFF: … and has the ability to make decisions in its own best interest that will also serve the national best interest, and where here the public includes local officials. I mean there are lots of people who need to understand what the capabilities are with various planning horizons, both before, during and after events in a way that that communication doesn't compromise us, so this is a technically difficult forum of communication that requires R&D.

MR. OXFORD: One other aspect that we talked about this morning on outreach is also reaching out to state and local governments to understand their needs. So this is getting into the community that may help provide us products, but reaching out to people so that we understand state and local needs. This is something we're beginning to work at the Office of Domestic Preparedness. We have a two-prong approach here that would be how to do business with small businesses and also how to get the requirements.

DR. BESSETTE: I think based on what I'm hearing, maybe we can expand to specify those areas such as Secretary Ridge's HSAC, the other governmental elected officials, agencies that could be part of the communications effort as well as the public.

GENERAL WELCH: Just to be sure you don't get bored, we rather casually said several times that you need to involve state and local officials in these forums where you're making decisions. The problem is I don't know how one does that. So when you

say state and local, you're not talking 50 entities, you're talking 5,000. The point is to give some thought to how you can actually get useful state and local flow in some way that's actually manageable.

DR. FISCHHOFF: It might be worth thinking about this as having two S&T elements: one sort of political element, where the S&T element is first trying to get the content right so that people understand what the issues are, and you understand what they're hearing; and one where you engineer the process (that's the research part of a question) and then implement it in a way that you've gotten the science right though it is probably in somebody else's department. You could provide guidance on how to have this two-way communication that is technically sound.

GENERAL WELCH: If you'll put a bullet on your chart that says that.

DR. BESSETTE: I take your point. Also, following on your point, General Welch, we did discuss in one of our meetings, as a matter of fact, taking advantage of Ernie's [Mitchell] skill sets to outreach to the first-responder community on a national basis and get their input into that. Is there anything you want to add to that?

DR. MITCHELL: I think we can flesh it out further, but there are a number of, let's say, large representative organizations that we could cross-sample to determine what the national consensus is, and take input as well as disseminate information. A lot of what folks are looking for is evaluation of technology, to see what works, so standards and testing and evaluation would be very helpful. I think we want to look at ways to get that involvement as well.

DR. BESSETTE: The last two slides, obviously, are based on our knowledge of the Department which has been increasing exponentially. Our methods of operation will be the same as other subcommittees, but based on the DHS missions, the subcommittee may utilize the following methods to assist our evaluation: by no means do we mean this is totally inclusive, but site visits would be useful to institutions engaged in research or manufacturing of product lines that might be important for us to learn more about; review of requested reports or other studies, both from government and other academic and industry sources, as well as on suggested methods for improved communications, as Baruch suggested. There are a number of studies that have already been done, but they need to be expanded on how to best communicate with the various publics that the Department deals with.

The last slide, in terms of what we saw as special issues, contains really two prime issues. As we said from the beginning, one of these is to assist the Department in identifying cutting edge technologies, and we thought these choices of words were important; that is, they are "realistic" (meaning the timetable), they are "reliable" (having sensitivities, specificities), and they are "practical" (meaning that first-responders and end-users or customers would find these helpful in enhancing homeland security). So in that bullet, we tried to capture the realism of budgetary constraints as well as the needs of customers to bring technology into their hands.

The second issue was assisting the Department to improve public communication. I think addressing Alice's [Gast] point there, we mean outreach public communications as a method for enhancing or improving homeland security. And I think Baruch has, obviously, a lot of experience in that area and can bring to bear how we should focus research to better improve the Department's ability to reach out to the public before there's an event. An educated public would be more secure than an uneducated public, and that, essentially, is how we viewed our missions.

GENERAL WELCH: Comments?

MS. BORRONE: I have a question of background information. You mentioned earlier the Secretary's Advisory Council (HSAC). There are a number of other activities that the Department of Homeland Security has underway that we might usefully learn about just to have this information or background. For example, I understand that there is a group that's been comprised of individuals from around the country who are experts in certain areas, that working through Louisiana State University could call upon experts in the case of an incident or an emergency. I don't know if it's called the SMART group, or whatever it might be called.

DR. VITKO: It's not through Louisiana State University per se. In the structure you saw for Weapons of Mass Destruction (WMD), Office of Incident Management, they have a group of subject matter experts that are called SMART. I forget what the acronym stands for, but it's sort of an subject matter expert readiness team, so in each of the areas they have a list of experts in biological, rad/nuc, and chemical that would scientifically support the Secretary; in the case of an incident, if somebody pulled an interagency incident management team, they would support it. So, yes.

MS. BORRONE: I'm just thinking, listening to what Russ [Bessette] is saying, that some interaction with the way they are thinking and approaching some of these issues with the work that you're describing might be helpful.

DR. BESSETTE: That would be a good idea and that would be a good place for us to either visit or communicate with them somehow.

GENERAL WELCH: Anything else on the committee?

DR. FISCHHOFF: One thing that's occurred to me in the course of these two days is that apparently there are a number of very different things that are called communications. There are public affairs, which to some extent speaks to the heart, perhaps more than the head, and that's kind of how to think about these things; there's the kind of routine, public health communications done by somebody with a bachelor's degree in communications studies – they usually aren't defense evaluated, are kind of best practices; and then there are other things that have to do with research done to make certain that the content of the message is worthy and is correct, which is often the problem with many of these because they're typical communications.

Each of these has its own rule for us to sort out, a lexicon of what are these things, what are the best practices in an area that we haven't been notably successful as a society and may not be what we want to endorse here. We may have an opportunity here to set the standards for better risk communications, or that we might find some good ways to figure out what's going on within the Department.

GENERAL WELCH: Well, we have time for any general discussion, but let me talk very briefly about some administrative items. The next meeting is planned in the Livermore Valley, 31 August - 1 September. It will be a joint Lawrence Livermore and Sandia Laboratory meeting. As I mentioned earlier, if you have comments regarding structure let me know so that I can inform the staff as to how we would like things changed. You have my email address as well as those of the staff. Other comments, questions, discussions? The meeting is adjourned.

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

Attachments:
Agenda
Attendees