# Summary of Meeting – Public Session

# U.S. Department of Homeland Security
# Homeland Security Advisory Council

## January 10, 2006

**Meeting Summary:**

This summary describes the discussions and recommendations of the U.S. Department of Homeland Security's Homeland Security Advisory Council (HSAC). The meeting was held from 10:00 a.m. to 12:00 noon on Tuesday, January 10, 2006 at the Mandarin Oriental Hotel in Washington, D.C.

The HSAC met in Washington, D.C. for the purposes of: (1) welcoming and swearing in new members of the HSAC; (2) deliberation on recommendations of the Critical Infrastructure Task Force and the Weapon's of Mass Effect Task Force; and (3) receive reports from Senior Advisory Committees.

**Participants:**

Council Members in Attendance:
Judge William Webster, Acting Chairman
Richard Andrews
Kathleen Bader
Elliott Broidy
Chuck Canterbury
Frank Cilluffo
Dr. Jared Cohon
Dr. Ruth David
The Honorable Thomas Foley
Herb Kelleher
John Magaw
Mayor Patrick McCrory
Governor Mitt Romney (via phone)
Dr. Lydia Thomas

**U.S. Department of Homeland Security Representatives:**

Secretary Michael Chertoff
Deputy Secretary Michael Jackson
Under Secretary for Preparedness, George Foresman
Assistant Secretary for Policy, Stewart Baker
Daniel Ostergaard, Homeland Security Advisory Council, Executive Director
Jeff Gaynor, Homeland Security Advisory Council Staff
Michael Fullerton, Homeland Security Advisory Council Staff
Mike Miron, Homeland Security Advisory Council Staff
Candace Stoltz, Homeland Security Advisory Council Staff
Carnes Eiserhardt, Homeland Security Advisory Council Staff

Al Martinez-Fonts, Director, Office of the Private Sector

**Public Attendance:**

Approximately 230 members of the public attended the meeting. The meeting was also carried live on CSPAN 2. There were many members of the Critical Infrastructure "Resiliency" Task Force in attendance.

***Homeland Security Advisory Council Meeting***
***Public Session***

**I N D E X**

**HSAC Meeting Called to Order at 10:05 A.M.**

**CHAIRMAN WEBSTER:** Good morning. Welcome to Secretary Chertoff and members of the council and members of the public to this 2nd Quarter Homeland Security Advisory Council Meeting. My name is William Webster, and I am Acting Chairman of the council. The Council serves to provide strategic policy recommendations to Secretary Chertoff and the Department of Homeland Security on a range of Homeland Security issues. We will be hearing some updates this morning from several task forces.

As a reminder to the public, deliberation and comments during today's session are limited to those briefing the Council and to Council members themselves. At the close of the public session, we will provide information on how you may provide commentary to the HSAC, as we call ourselves, and the Department of Homeland Security.

It is a great pleasure to welcome all of you to this session and especially to welcome the Secretary of Homeland Security, the Honorable Michael Chertoff. Judge Chertoff, we are very pleased to have you here. Would you care to comment?

**SECRETARY CHERTOFF:** Judge Webster, thank you. I am delighted to be here at what looks to be a replica of the Congress in Vienna. I am also astonished at the number of people who are here, given that there is a hearing going on across town. So, I guess there is an infinite capacity for people who are attending meetings.

I am delighted, first of all, to welcome three new members to this Council. One is Ambassador Tom Foley, a former Speaker of the House, who is seated to my left. One is John Magaw, former head of the Secret Service, and Elliott Broidy, who is a distinguished businessman. I think these individuals add further depth to the bench that we bring to this Council, which is the -- of all of the various we have to intersect with a wide variety of wise people, probably the premier venue as far as our department is concerned.

We begin the New Year after what was certainly a year of tremendous challenge. A year that challenged us in terms of our preparedness challenged us in terms of our efforts to control the border and challenged us with respect to our continuing desire to adapt technology in order to protect ourselves from terrorists or other people who want to come into the country and do us harm.

The passage of the New Year does not eliminate these challenges, but it gives us an opportunity to take a deep breath and consider what we have learned and how we might improve ourselves as we go forward. I look forward to working with the members of the council and the subcommittees in this coming year, adapting lessons learned and applying their wisdom to how we can make ourselves better going forward.

So with that, I look forward to hearing the reports as they come in. I am going to have to excuse myself at 11:00 because I have something that I have to attend, but I will certainly read what I haven't heard in the next few days.

**CHAIRMAN WEBSTER:** Thank you very much, Mr. Secretary. We will now proceed to the reports of the subcommittees who have been working on task force reports and deliberation. The first of these is Weapons of Mass Effect. Our Chairperson is Dr. Lydia Thomas, and her Vice Chair is Jared Cohon.

***Weapons of Mass Effect***
***by Dr. Lydia Thomas***

**DR. THOMAS:** Thank you very much, Mr. Chairman. Good morning, Mr. Secretary. It is my honor and privilege to report to the HSAC this morning and to you, Mr. Secretary, on the workings of the task force set out by the HSAC on the topic, "Preventing the Entry of Weapons of Mass Effect into the United States."

The purpose obviously is to look at a prevention strategy, or to help develop a prevention strategy, such that not only the weapons, but the components of these weapons, as well as the individuals who may use them, would be acquitted well.

The scope, I should mention, included not only our traditional notion of weapons of mass destruction. The Lexicon project notwithstanding, it is not the intent of the task force to increase the confusion level. But we thought it was very important that we indicate that any time you could cause grave destruction, psychological or economic damage, using chemical, biological, radiological, nuclear or explosive devices, they would indeed be included in this study.

In other words, the cause of an extensive loss of life or property was not necessarily the driving influence here. We wanted to be more inclusive and over-define, if you will, mass destruction, and thus, the term "Weapons of Mass Effect." We did exclude form the study cyber threats, because they were being conducted elsewhere.

One of the big tasks, as it turns out, for us was just defining the word "border." Initially it sounds like a very easy concept. You know, we think about the confines of the United States; the map that we all learned as children. But when you really begin to think about it, the physical border is only one of our borders.

There are institutional borders, such as the Air Defense Identification Zone. There are the facility based borders, and the most obvious example of those would be the international airports, many of which are located far into the interior of the country. But indeed for people entering, legally or otherwise, that is their first opportunity to be on American soil.

We think also that while there are three parts to the prevention effort, clearly neutralization of the terrorists would be one part. Securing the weapons, securing the components of the weapons, a non-proliferation strategy, is also a very important part of prevention.

We were not concentrating on those, per se, but concentrating on the entry mode. That is, actually going from the origin of the threat into the United States. We also excluded consequence management.

The members of the task force are listed there before you. It was an extremely dynamic and engaged group. We had many meetings, which I will point out in just a few minutes. But they are there for your review, and I am sure that any one of the members of the task force who are here today; I hope that you will chime in at any point when you feel that there is some information that should be conveyed that I have neglected in this brief presentation.

In order to address the charge to the task force, we had to develop an approach. And while we recognized that trying to disassemble prevention as a program into components parts would always be a somewhat difficult task, we had to find some way to bisect, dissect and, in this case, trisect the problem in order to try and get our arms around it.

We were very fortunate to have three members of the task force who agreed to serve as subgroup chairmen and to look at the corridors of entry of weapons of mass effect, as well as the individuals who may use them. Those individuals were Norm Augustine, who handled the air corridor; Jim Schlesinger, and land corridor, David Abshire, the sea corridor.

We then proceeded to go into a very extensive information collection process. As you could well imagine, we wanted to have the best baseline that we possibly could, and so, we talked to many, many experts at the strategic, the tactical and the operational levels of not only the Federal Government, but state and local governments.

We spoke with individuals who are representing our allies, who have similar homeland security responsibilities and we talked to a number of individuals in the private sector who are themselves homeland security experts and who see this as very much a part of the survivability of their businesses.

The presentations were given on both threats and vulnerabilities and the current systems and plans, at a total of 12 meetings that began in March of last year and concluded in October of last year. We were a very busy and very active group.

We then got to the very difficult part, and that was the analysis phase. We wanted to assess the information that we had on the threat, the current systems, the plans that were in place, the practices in place for WME prevention and then to develop recommendations to present first to the HSAC and then, with the agreement of the full body, hopefully, sir, to you.

Getting to the heart of the matter, clearly this is all driven by the threat, and an attack on our country WME is clearly the gravest danger to American national security. Different WME scenarios, the use of nuclear or biological, radiological or conventional weapons against U.S. targets will have different likelihoods and different impacts, including perhaps the number of civilian casualties that we would sustain.

But regardless of the scenario that we looked at, the consequences are almost unimaginable, and therefore, we believe that preventing weapons of mass effect and their use on U.S. soil by individuals who would seek to harm us must be our most urgent priority and the subject of a focused and integrated effort. We believe that this is a very grave concern today, and we have to address it.

In terms of the consequences that we looked at from the threat itself, we came to the consensus, shall I say, that nuclear weapons comprise the greatest threat against America by a terrorist organization, because an explosion of even a very low yield weapon in a large city, such as New York, Boston, Philadelphia, cities on the West Coast and cities in the Gulf, would no doubt result in hundreds of thousands of casualties immediately and then probably that same order of magnitude in the following days.

Even though we realize it is the most catastrophic, we still believe, based on the expert presentations that we received, that it is probably the lowest probability for a number of reasons. But nonetheless, one that we in no way can ignore, and that is one of the reasons that we believe that the new NDO Office is so important and the work that is going on there. I will get back to that in just a second.

One thing that was very clear as a result of the presentations that we received and the discussions that entailed was that we have made a lot of progress. Obviously, one of the very first things is that the Department of Homeland Security was formed, and it is really starting to come together, and that there is the Homeland Security Council that is supposed to look at the highest policy level; at how we are doing as a nation.

We are also heartened by the new Policy Office within the Department of Homeland Security; an entity that we believe was sorely needed. It came up in your second stage review and has now been implemented.

Lots and lots of programs are underway; great programs that we were privileged to hear about in a great deal of detail. The Container Security Initiative is just one of them. There were many. The Mega ports Initiative that is being conducted by DOE is yet another and the fact that we are starting to get some of the infrastructure in place that allows us to handle these situations. We were taken out to see a number of the Command Centers around the country.

I think the probably the most impressive thing of all was the dedication of the people themselves. Whether they were coming from the Federal Government or the state and local governments or the private sector, people who are every day working these issues and these problems are working very hard, are very capable and very dedicated to getting this right.

We did, however, find what we believed to be some critical deficiencies in our prevention strategy. Number one, and the most glaring, is the absence of an integrated systems approach to the entire problem. And when I say the entire problem, I mean those three phases that I talked about: Neutralization of the terrorists, non-proliferation of the weapons or their components, as well as being able to prevent people or the weapons from entering the country.

There was also an absence of a systematic risk based approach to the investment. While we commend the department on the risk based approach now to the allocation of the grants fund, we believe that a risk based system, as I will talk a little bit more about later, is an approach for the department. But it is certainly a great approach for a prevention system, because clearly, the best way to not to have to deal with cleanup, preparedness, mitigation is to not have this occur to begin with.

Another somewhat distressing element was the fact that while we found good capabilities existing, capabilities being developed, we found strong leadership and we found decision making is very dispersed. Almost every element of what you need to put together a prevention program is spread across the Federal Government, spread across state and local governments, spread across international entities, international bodies, and the coordination is lacking.

Looking at deterrence we found what we believed to be an inadequate engagement of our foreign partners. While there is some good work on when you look at some of the container security work for instance or some of the good work of TSA and that of our immigrations operations, we still believe that this is a global problem and that the department and the nation are not yet fully engaged at the level with our foreign partners that we need to be in order to get our arms around this.

We think we have some fairly outdated deterrence concepts. We have a tendency quite often to drop back into our Cold War mentality when the enemy was very clear and what we were facing, namely nuclear weapons, very clear. It is not the situation that we face at all today, and it really requires a fresh look and we have some recommendations along those lines.

We think there is a lack of sufficient urgency and priority in the technology innovation arena in particular. During some of our discussions, just as an example, an individual mentioned the fact that when the country decided to go to the moon, we did it. We put the resources behind it, we put the best brains we had behind it, we worked and we got there.

This mission is much more important in many of our minds perhaps than that one. Not saying that it was not a great national accomplishment, but we figured that if we can do that, we can do this. But it takes the same kind of drive, it takes the same kind of urgency, it takes the same kind of raising of the national consciousness so that you can get everybody behind it.

And that brings us to the last point, which is the citizen engagement. Even in the prevention arena we believe that citizens of this country have a great deal to offer, and we have recommendations along those lines.

This then brings us to, okay, so how do you start to get your arms around this? And we put together a conceptual framework, a systems view, if you will, because we believe that the overall prevention effort is indeed a system that you can look at from that standpoint.

There are the three thrusts, as I mentioned. The neutralization of the terrorists, which is ideal. Then next in line, securing the WME, and then the subject of this task force, which is detection and interdiction in transit.

We know that if you are going to think about detection and interdiction in transit, that there are three dimensions of the problem that you can think about that help you develop an approach, and that is the geographical, the spatial dimension, the functional dimension and the operational one.

To decrease risk of a successful WME penetration of U.S. borders, you want to design a system such that its effectiveness is as close to the origin of the threat as you possibly can. This diagram was our attempt at least to try and visualize what we were talking about when it comes to the geographical dimension.

If you look at the threat as it is presented there on the far left hand side of the screen and the target being somewhere within the U.S. borders, on the right hand side of the screen, you will see that once you get much further out than the threat itself, which is the reason that makes neutralization of the terrorists so important, the space greatly expands and we have the potential of the needle in the haystack issue, which makes life very complicated and very difficult.

But we know that if you look at these three corridors of entry, once you get past the national borders and international borders, you can look at the root crossing many of these corridors.

In other words, even though we segmented air, sea and land, you could imagine a threat originating on land, being transported by air, then by sea and then once again by land before it ultimately reaches the target. As a result, the system itself must be extremely flexible in order to be able to deal with it.

The functional component of the whole strategy entails these areas where, if you start going around the circle, and I won't go through all of them for sake of the time, you could start thinking about a prevention strategy that has a component of dissuasion as one of its functions. You want to get at the radicalization that is going on and turn that around as best we can.

New social policies; the moral ground. In other words, let's not continue to create terrorists. Then you get to the notion of deterrence.

The more things that we have out there that may indeed cause a terrorist to believe that they could fail make a big difference. So, we looked at spoofing. We looked at making sure that we are not predictable, changing the way we go about doing things and changing the way we inspect and those sorts of things.

Then, of course, there are all of the traditional ones, detection as well as the new things that we would like to see come along, in addition to denial which, in essence, prevents access source materials, prevents access to knowledge, expertise, consequence, rich targets and all of those kinds of things, coming full circle to elimination, which would obviously be the ideal. That is, no terrorist threats to our country.

The second dimension of the strategy would be that of institutions who would go about taking care of these functions and looking at the geographical dimensions. And what tools would they use? And we put the tools that we believe are important to the overall strategy into three buckets, if you will.

Transactional tools, which would include things like process associated with purchasing and shipping and travel. Informational tools, the information collection that goes on. Operational information. Then, of course, the technological tools, which would be things like identity management, using biometrics, data mining and other detection technology, such as sensors and detectors

Putting this in a systems concept that has all of these elements we believe allows the owner of the system, if you will, the owner of the WME prevention system, to ask some very fundamental questions. These are just examples. I apologize for the busyness of the chart, but I thought it was important to try and make the point that when you take the systems view and the systems perspective, that you can ask yourself some of these questions and make, hopefully, the best decisions on behalf of the country.

So, what should be the relative balance of investment for the three basic thrusts? That is, neutralizing terrorists, securing potential WME sources and detecting. When we make these precious resource allocations, we realize we don't have all of the money in the world to throw at all of them.

So, when you look at the system, how are we going to get the best bang for the buck? Given where we are today, where should those allocations be made? Because the whole notion here in taking this systems view is a risk reduction process. We believe that, unfortunately, coming to zero is probably unrealistic, zero being one of those nice mathematical concepts that rarely exist in real life.

But we believe that with a system view you can do better allocation schemes. You can certainly prioritize where you want to get the work done and you can ask all of the right questions because it is all there in front of you.

Getting to the risk reduction and how important that is, we believe that a risk reduction analysis should be structured to address the fundamental choices available to the country in confronting the WME prevention challenge. Each option representing different combinations of policies, organizations, technologies or processes should be addressed in terms of its benefits in relation to its cost, and ultimately, the benefit in terms of risk reduction is the most important measure of value.

We also believed, in addressing the risk reduction process, that this is a politically difficult arena that I am sure that you are more than familiar with. But we believe that once we make it clear to all of the stakeholders in the process that this is the best net benefit approach for the country, we will get the support across the board that is required to make some of these very difficult tradeoffs.

One of the things that we were most concerned about is the tendency to spread our precious resources, dare I say almost like peanut butter, and I don't mean that is an overly cavalier statement. But it certainly is something that we see all too often.

We believe that the -- in order to conduct this risk based approach for prevention, somehow we must find a way to protect the budget. First, develop it mostly from top down based on this risk reduction approach, such that the monies are going to the places that are really needed and really will give us the value that we are seeking. But also, protect it such that it can't be amended.

I know that is a very tall order. We struggled, sir, quite a bit with how we could help you. One of the things that we thought about, even though it is clearly not a perfect analogy for this situation -- but because we realized that once a risk approach is applied there will invariably be winners and there will be losers, there will be the temptation to get everybody into the winners' category.

We would like to find something that is the moral equivalent, if you will, of a BRAC (sic) process. We are not saying that we -- someone who can say this is an up or down. You know, the department and all of its sister agencies that are involved in this have decided that these are the elements, these are the locations, these are whatever that falls within your overall prevention strategy risk reduction scheme. This is what we need to do.

It is up or down. You can't just sort of slide this place in and slide that place out. These are the things that we must do and it is all; you take them all.

We are prepared to continue to work with you to come up with something that is perhaps better, but I hope that you get the point. We would like to help you, sir, because we know what a difficult political challenge you are facing.

In addition to the risk reduction, when we look at our corridors of entry, when we looked at the geographical, the landscape issue if you will, then we overlay that with all of the functions that one could conduct along that landscape, and then when we look at the whole risk reduction approach, we believe that a system that we have used many times in the past very successfully is one that could be used again.

We have layered, if you will, our defenses and we can layer the prevention strategy. If you just think about things like nuclear power plants and nuclear safety, for instance, there are geographical elements in terms of perimeter protection and that sort of thing. There are biometrics and careful screening of the individuals.

So, there are lots of tools that are employed, there is lots of redundancy and backup safety systems, such that even though we may sustain a failure, it is not a catastrophic failure, because there is another layer of protection there. We have done it in Strategic Nuclear Defense. We have done it in conventional warfare. We can just look at how naval battle groups are constructed for instance. It is a layered defense type of a system.

And the rest of them are there for you to peruse, because we believe that we can glean a lot for our prevention strategies from some of these lessons of the past. The important thing is that they give us the redundancy, they give us the flexibility.

It gives us the robustness that we need, such that we don't have these single point failures, we don't have the catastrophic effects, and indeed, the layers themselves can be cumulative, if not duplicative, if they are constructed correctly going across the geographical, functional and operational approaches.

That said, we had some very specific recommendations. In its current state we believe that WME prevention is critically flawed and must be improved and that the various elements of WME prevention do not work together as an integrated system to achieve the strategic functions of WME defense.

Resources are not systematically allocated based on their contribution to risk reduction. We can't say that often enough.

Improvement is urgently needed, and given the catastrophic potential of a WME attack and considering the deficiencies in the current defense and the features and value of a layered WME prevention system, the task force identified four major areas for improvement.

The first area is in authority, alignment and incentives. We very strongly believe that we need to clarify and strengthen the role and authority of you, Mr. Secretary, and of the Homeland Security Council. I want to put a point there. There is quite a bit of that in the text itself.

We believe that the Homeland Security Council should be on a par with the National Security Council. Failing that, it should be perhaps a part of the National Security Council, because we believe that prevention of an attack on the United States, as well as all of the other aspects of homeland security that you guys deal with, must be priority number one and get the same level of attention, direction, policy, awareness and support that items coming out of the National Security Council receive.

Having it a part of the Act is a great thing. Now we have got to put the muscle behind it. Not them managing you, but in that very top level policy and priority.

We also believe that in order to take this as a system, to do the full integration, you have got to have somebody in charge, and we think that there are a number of role models out there that we could adopt for this one. We have seen joint program offices, for instance, in the Department of Defense for many years. It is a model that works for them very well. It allows you to place people in it from multiple agencies and that sort of thing.

The important thing I think is that once you get that system view the important players are brought together and there is someone responsible for making sure that the strategy is carried out.

We believe that you need to engage internationally, as I mentioned, the specific recommendation being more emphasis in the department with people who are trained and have, as their specific job, interactions with our allies who have also a homeland function.

We also believe that it is very important that the State Department -- and I realize, Mr. Secretary, that you don't want every agency in the Federal Government, and I apologize for giving you jobs that you may not have the authority over, but we think it is important to get these things on the table and that in your discussions with the President you relay what your council has suggested to you.

The State Department has, to our understanding, no individuals who have as their sole function in U.S. embassies and consulates around the world, homeland security that is job number one for them every day. There are many people who have that as an assignment, but we believe it is too important to be as just another assignment in a very long list of activities to be conducted by our diplomatic corps. We need people on the ground from the State department for that being job one.

We also believe, going back to this whole joint effort business -- and this was really brought home to us by people who have been very involved in joint efforts. Norm Augustine. So was Jim Schlesinger.

If you really want people to work together and to be well aligned, then you reward -- first you put them together and you reward them for jointness and you do as much interchanging as you possibly can; moving people around; rewarding them for being a part of a joint activity, as opposed to their parochial activities in their home stovepipe.

We realize that is a very natural tendency. If you stay inside the stovepipe, that is how you think. If you are outside of it and you are forced to think across the board, it is remarkable how well people adapt to that situation, and we have seen it work many times in the past.

No doubt that we need to improve WME intelligence. That was brought out over and over and over again. And one of the things that we believe is very important to continue to push on is that the Department of Homeland Security must be a principal at the table when our intelligence efforts are being developed. You are a very big customer of intelligence in this arena, and you have got to be a full partner.

We also believe that we need to clarify the role of the Defense Department in disaster response, and there are two reasons for that. You say this is prevention. Why are we talking about the Defense Department disaster response?

Number one, we think it is a huge deterrent. If you just think back to our unfortunate times very recently as a result of Katrina and Wilma and Rita, if that had been a terrorist attack instead of a natural disaster and we had been able to execute all of the things that we would like in the fashion that we would like, in, in and of itself, is somewhat of a deterrent to terrorists.

Why would you want to do something when indeed -- it may be somewhat disrupting for a little while, but we are resilient people. We have the ability to rebound. Our infrastructure hangs in there. You know, people are taken care of. It is the image that we must portray. Not only because it is the right thing to do, but because we believe it is also deterrence, which then brings in the exact role of DOD.

And we recognize that, once again, we are dealing with a political problem, as well as a legal problem. The Department of Defense has certain limitations with regard to its activities within the borders of the United States, yet it is also abundantly clear that is, as an agency, has many very unique features and capabilities that may indeed be brought to bear, if indeed there were a national disaster of some significance.

And so, we believe that getting those rules straight, how this would plug-and-play, how it would work with the Governors and the state and local people is important to have straight now. You know, what capabilities are we talking about? When would they be called in? When would the Governors be willing to accept that kind of assistance?

And how does it mesh with what the department would be prepared to do is, we believe, a very important aspect of response. But also, a very hard driver in our -- the way we look at deterrence.

Updating deterrence. Some of these have real policy flair. We think we need to make our deterrence policy clear. Most of the task members were adamant about this, in that we need to reiterate our policy of swift, certain and severe consequences for any nation associated with terrorists using weapons of mass effect.

We believe we need to expand our deterrence by putting in place this layered defense system that I described earlier. It just give us, we believe, what we need to increase the likelihood of failure, if indeed there were an attack.

We think that we could also engage the citizens of the United States. One of our members in particular,

Dr. Abshire, is very strong on the use of an entity that he calls a "Home Guard." He believes, and many of the members of task force also believe, that people in this country would very much like to participate in securing the homeland, if indeed we could tell them what we want them to do.

We believe that there are some roles that they could take on, particularly in the aftermath of a disaster. Once again, allowing us to be able to recover much faster and, as a result, indicating another facet of deterrence.

The other leading recommendation falls into the category of that whole idea of instituting a risk-based process for resource allocation. I talked about that quite extensively already. So I won't go back through it again. But you will find that there are a number of recommendations in that arena within the report.

And then, to improve across the board the private sector contribution to the process of risk management. I know it is old news and we all say it over and over again. Most of what we are trying to protect does not belong to the Federal Government. It is in the private sector.

The numbers vary from 75 percent to 85 percent, but nonetheless, it is the lion's share. And when we were discussing homeland security with many individuals from the private sector, whether they were in the trucking industry, the shipping industry or many other areas, we found that they had some very, very good ideas. And if we found a way to form better partnerships, we could really benefit from that knowledge.

There are some examples of that that are working out fine already. We believe that there are many more that could be instituted.

Instituting the systems management effort. Putting together either a joint program office or something to that effect would be important.

We believe you need to make innovation a real priority, and I talked about that. Get the urgency out there. Get people focused on the things that we still need to do. Improving our detection capability and that sort of thing.

Bringing our research community really to bear on problem number one, and that is making sure that we can, to the best of our ability, detect any attack on our homeland.

And we believe that we can encourage and nurture some of these ideas. There are lots of models for that sort of thing. We talked about the Incutel model for instance. Not that you should necessarily repeat that one, but sometimes taking things slightly out of government could facilitate some of the innovation. How we go about doing things, how it gets supported and that sort of thing. Looking for some more out-of-the-box thinking, if you will.

Within the report we have some very specific actions. We realize that we are having all these nice global thoughts about things that are very difficult to do. It is good, but not particularly useful.

And so, what we tried to do within the report is to give you some very specific examples of the kinds of things that you may want to consider in order to address some of the recommendations that we made. We looked at the Telecommunications Advisory Committee, for instance, as the kind of entity that you might want to establish to get better input from the industry.

We also have a very extensive set of appendices in the report where there are other ideas and observations that we developed over time throughout this process. An example there is one of the gentleman that we spoke with from the transportation industry, particularly, the trucking industry, told us that his truckers involved in international transport have six background checks from six different organizations.

There must be ways for us to operate more efficiently. I know you are very well aware of that. The trick is to find them all and then developing the policies and the budgets around them that will support giving us better efficiencies and better ways to operate.

The very last thing that I wanted to do was just to thank everybody who worked extremely hard to try to present you with a set of recommendations and actions that you could take to improve our prevention strategy as we see it. Those individuals came, as I said, from government, state and local, and from the private sector.

Lots of agency heads hosted us at a variety of venues. We had a very strong and active writing team, and the task force members were not at all shy about telling us when they thought there were some really good ideas on paper and when there weren't.

So, we are hoping that the final report that we do provide to you in the next couple of weeks will be beneficial. We have enjoyed the work, and we certainly hope that there is some good coming out of it.

**CHAIRMAN WEBSTER:** Thank you, Lydia, for a very full and comprehensive report. Mr. Secretary, I know that you have to leave. Do you have any response that you wish to make?

**SECRETARY CHERTOFF:** I do. First of all, I want to thank you for what is an exhaustive review of the subject, obviously reflecting a lot of hard work and some very good ideas and some useful suggestions.

One of the things that I am pleased to observe, in fact, is that a number of the things recommended are things that we already have underway in some way or another. I couldn't be in greater agreement, in more violent agreement, with your principle of risk approach to funding.

And as I have seen in the last couple of weeks, there obviously is a political cost. I don't know if I am quite ready to say we ought to do a BRAC. I guess I'm the BRAC.

**DR. THOMAS:** We didn't think you would be.

**SECRETARY CHERTOFF:** I guess I'm the BRAC and I have to take the heat for the decisions. I do think that we want to be as transparent as we can be. We have also adapted the concept of layer defense, as you know, in a number of areas with respect to our maritime domain where we do things starting overseas through our continued security initiative. We then do targeting through the Coast Guard for vessels coming in. We do things at our ports. I think we are very much onboard already with that.

As you observed, our Domestic Nuclear Detection Office is a joint program office, and that is a good example, at least in the nuclear area, of using this approach. And likewise, we are pursuing the ideas of having DHS attaches overseas and building the concept of jointness into our career development paths. So, many of these are recommendations which I think are very consistent with things that we have underway.

I would ask you to do one thing. I think everybody in the Administration is in full agreement with this notion of an integrated systems approach. Of course, the Homeland Security Advisory Committee looks at the Department of Homeland Security.

As you know, the WMD Commission made a series of recommendations specifically addressing the issue of weapons of mass destruction, which is a subset of weapons of mass effect, and talked about the idea of setting up a national counter proliferation center, which would be the integrator of this entire system.

That was adopted by the President. Ambassador Negroponte, the Director of National Intelligence, has the responsibility for getting this underway and is, in fact, doing so. We are working with the DNI and the other major players in this in setting up this joint effort.

I wonder if you would consider whether, in fact, this national counter proliferation center under the DNI and this approach adopted under the WMD report essentially achieves the result you are suggesting here. Not necessarily within the ambit of this department, but by looking across all of the departments.

And it is a publicly available report, and I think all of this is on the web. So, that would be helpful in terms of calibrating what you are recommending against what is under way in another part of what we are doing.

That being said, as I said earlier, I have to go off. But nothing is more important than dealing with this issue. There are a lot of, I know, specific suggestions that you are making. I am going to look forward to reading this and responding, particularly after you have taken into account this one request I have made.

I don't know if the Deputy has more to add. I am going to leave you. I look forward to continue to work with you.

**DR. THOMAS:** I was just going to say that we did look at the report, and I think perhaps what would be most useful is a short summary of where the overlaps are and where the differences are, because we did add a little more.

**SECRETARY CHERTOFF:** That would be perfect. That would be terrific. Thanks very much.

**CHAIRMAN WEBSTER:** Thank you, Mr. Secretary. We appreciate the time you have been able to give us.

We are delighted that your deputy, the Honorable Michael Jackson, has joined us and will be responsive, I assume to the extent he is able, to the remainder of the task forces. Do you have anything that you would like to say?

**DEPUTY SECRETARY JACKSON:** Not at this point, Judge. Thank you.

**CHAIRMAN WEBSTER:** Okay. We will move right on to the next task force, which is the Task Force on Critical Infrastructure, chaired by Dr. Ruth David and her Deputy, Mr. Erle Nye. Ruth, the floor is yours.

## ***Critical Infrastructure Task Force***
### ***by Dr. Ruth David***

**DR. DAVID:** Thank you, Mr. Chairman, Deputy Secretary Jackson. Let me first say that you will hear many recurring themes from the presentation you just heard from Dr. Thomas. An emphasis on systems thinking, system approach, holistic approach, risk management and so forth. I think we are very well aligned.

If I might, I would say that the previous task force looked at things from a weapons perspective. We are looking at things from a target perspective, in a sense, by looking at critical infrastructures.

I would remind you of our original charter, which was to focus on advancing policy and strategy at a very high level, and we retained that focus throughout our deliberations. We certainly collected a lot of examples and anecdotes that we believe could influence near term actions.

But in developing our recommendations, we tried to maintain a focus on the top level strategy and policy. One of the things we went into this effort with was an appreciation that this is a very complex topic. Certainly throughout our deliberations we learned more about just how complex it really is, the diversity of the stakeholder groups.

Unlike dealing with issues such as weapons of mass effect or weapons of mass destruction, which has been, to date, largely a Federal Government responsibility, when we start talking about critical infrastructures we bring in stakeholders not only at all levels of government, but certainly, as Dr. Thomas mentioned, the private sector who owns the bulk of this target set in a sense.

We ended up in our report with six, I will say, top level recommendations, each of which has a few subsidiary or subordinate pieces to it. But we really did try to stay at a high level. In our report though we also included as appendices some White Papers that provide examples either of ongoing initiatives, which we found greatly illuminating, and frankly, quite encouraging, or things that the department might think about in terms of advancing the state of play.

Rather than disassembling what we heard and imbedding it in the report, we chose to include those examples as appendices so that you could see intact some of the thinking that is going on throughout the country.

If I could turn to the membership - We did have a very diverse group of folks on this task force representing virtually all of the different key stakeholder communities, which turned out to be very important throughout our deliberations and discussions.

In addition, however, we were aided significantly by subject matter experts drawn from the government and also from the private sector, as well as from the research community. These folks brought a lot of talent to our discussions, and we certainly are in their debt.

Our task force actually met in person four times, and again, I would like to offer my thanks to the folks who hosted those meetings. At each meeting we tried to take a little bit of a different slice of the problem.

So, our first meeting in Charlotte I would say was really a focus on getting the state of play, hearing from the Federal Government perspective what was happening with critical infrastructure programs, but also, hearing about some of the international initiatives in particular, focusing more specifically on critical infrastructure resilience.

At our next meeting, which we held at the Naval Postgraduate School, we intentionally did a sampling of various sectors, the critical infrastructure sectors, and we tried to get representatives from as many different types of sectors as possible. As you well know, one of the challenges in this area is that each sector has different characteristics in many regards.
Some of them are tightly coupled intra dependent. For example, the financial and banking services sector. Others are, at best, loosely coupled; food and agriculture. So, within the sector they don't have the same strong cohesion as the banking and financial services.

We also wanted to do a sampling about interdependencies between the various sectors. For example, you see that virtually every sector is dependent, in some measure, on energy and on telecommunications and on transportation.

So what we were trying to do is get a sense of the overall complexity. When we talk about planning and policy for critical infrastructures, it is to look at that diversity and say how we develop a framework that is applicable across the diversity.

We also spent a couple of one day sessions being hosted at the Federal Reserve, and here again, the focus was learning about initiatives. For example, the Federal Reserve initiatives that had been in place for many, many years. Very, very mature. Focusing on maintaining continuity; on resilience of our system that underpins the finances of the country.

We also began to bring in examples from regional and local initiatives, again, focusing on resilience. And that, I guess, is going to be the theme of the rest of the presentation; is what we believe is a need to turn the nation's focus. Not at 90 degrees, but to vector the nation's focus from what has been called critical infrastructure protection to critical infrastructure resilience. I am going to spend the rest of the time building the case for doing that.

I wanted to start by sort of looking back at history. Actually, if you look even predating the time line that is shown here, a couple of decades prior to this we began focusing, in a sense, on critical infrastructures relating to the need to maintain continuity to our constitutional form of government. The so-called COOP and COG programs; continuity of operations and continuity of government.

That really stemmed from a need to maintain continuity incase of a nuclear attack. Those programs carried through to, basically, the late '80s and early '90s. With the collapse of the Soviet Union we began reducing emphasis on those programs. But at the same time, our nation became increasingly dependent on information technology and on interdependent information networks.

So what we saw was a rising concern about new kinds of vulnerabilities. Not just the threat of nuclear attacks, but new kinds of potential threats to our nation.

It is very interesting, because if you look at the original executive order issued back in 1996 that was titled "Critical Infrastructure Protection in the Information Age." It actually identifies continuity of government as one of the critical infrastructures. So there was sort of an alignment of interests, but a shifting in terms of the type of threat that we began to focus on.

That same executive order chartered a presidential commission to begin looking at the issue of infrastructure protection, and the result was a president directive, PDD 63. That was issued in 1998. We saw throughout the subsequent years shifting attention depending on what was happening, in a sense, to our nation.

As we approached the year 2000, we, of course, shifted a lot of attention to dealing with the software glitch, the Y2K bug. During that era I think it is noteworthy to observe that there was significant public/private sector partnership built up around insuring continuity through the Y2K transition. A lot of information collection mechanisms were put into place. A lot of relationships were developed around dealing with that particular issue.
Now, I will observe that it had the advantage of occurring on a date certain and having a very readily identified threat that we were dealing with. So, there was a focus of attention that I think greatly benefited the planning activities.

Subsequent to that we saw the next sort of shockwave into the system, which were the terrorist's attacks on 9/11. And with that, in a sense, the attention shifted back from focusing more on cyber to focusing more on physical protection of assets, although I will say that the planning for the two continued somewhat in parallel over the next couple of years.

In fact, there were two plans that were issued out of the Office of Homeland Security. One for the national strategy to secure cyber space and another for the physical protection of critical infrastructures and key assets. The theory was that the national infrastructure protection plan would bring these two together and build an integrated approach.
But I want to step back and say throughout this entire period the semantic focus was on the protection of critical infrastructures, and the threat against which we were protecting was terrorism.

If we could turn to the next chart, I pulled what was articulated in PDD 63 as a national goal. Now, I remind you this was back in 1998. There are a couple of things that I think are noteworthy in this.

First of all, it has some time lines in it. Secondly though, it does focus on protection against intentional acts. Now, it is a little bit beyond terrorism, but it still is a focus on intentional acts.

The other thing this goal does though is identify broadly the three key stakeholder communities, and I think that is very important. The Federal Government has certain things that it needs to accomplish, state and local governments similarly, but the role of the private sector is also articulated in that national goal.

What I have highlighted at the bottom though I think is the interesting point, because I would argue that the final sentence of this goal is more about resilience than it is simply about protection, and that is going to be at the heart of our discussion today. Unfortunately, in the subsequent years this goal perhaps was overtaken by events. But nonetheless, there was not discernable action that was taken in regard to achieving this particular goal.

Let me move on to the task force recommendations. I want to emphasize particularly our first recommendation, which some may view as simply a semantic argument. We see it far more importantly than that. I have observed the emphasis to date that has been on protection. My fundamental argument is that protection in isolation is a brittle strategy. If protection fails, what next?

So the argument that I would make is that resilience is a higher level strategy. You must have an element of protection to achieve resilience, but you can devise protective strategies that will never deliver resilience. So, our basic argument is that resilience is the appropriate outcome, if you will. It is the outcome we seek, not simply protection.
Now, you will see that many of our plans, which are entitled "Critical Infrastructure Protection," do access appropriately threats and consequences, which they must in order to identify, in a priority sense, which vulnerabilities must be reduced; which are the most critical to address.

Nonetheless, the focus of action has been on reducing vulnerabilities, because that is what protection is about.

We offer this definition, which we actually pulled from *Science Magazine.* "Resiliency is defined as the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must."

I think to drive home this point I would offer an anecdote that was shared with me by a colleague some months ago. The story is that in the very early days of the phone company there were very serious problems with backhoe operators who continued to dig up phone lines severing connections.

The phone company first did all of the traditional protective activities. They armored their cables, they posted signs, they put out maps; all of the warnings they could think of. "Don’t dig here." Nonetheless, it keeps happening.

So, they put in a secondary strategy, which was to immediately detect an interruption and reroute traffic instantaneously. That is the difference between resilience and protection. It is not that you don’t protect. It is that that, in isolation, is insufficient.
I will argue that a strategy that focuses on resilience is a necessary integration of all three components in the risk equation. You do what you can to reduce the threat. You do what you can to reduce vulnerabilities or to protect, and you do what you can to mitigate consequences, should it occur.

So, it is a balanced approach. This is not a replacement for risk management. This is the outcome from good risk management in our minds.

Our rationale I think is quite simple. One is we believe resilience has a clear and quantifiable target that could be set. It is the time, the time required to restore full functionality, should a disruption occur. So, there is something very tangible that you are seeking to measure in this case.

We also believe, and this is based on a lot of conversations with private sector representatives -- we believe this approach is very, very well aligned with the private sector is headed at this point. Whether they call it continuity of business or enterprise risk management, it is really all about taking a holistic approach, a systems approach, looking at every aspect and making sure that you can maintain your activities regardless of what happens.

The other point that I would make -- one of the issues that Dr. Thomas pointed out is that most businesses today, most governments today, most anyone today doesn't control all of the assets upon which they depend. So, putting into place planning structures that assume you may lose access to certain assets and build in the resilience, the ability to deal with that. It is far more robust than the notion that you can protect everything on which you depend. The final point that I would make is that, again, it goes back to words are important. We are seeing a growing adoption for the term resilience, both nationally and internationally. In the appendices to the report you will see some examples of local and regional initiatives along these lines.

I would point out that the United Kingdom also has just issued a report talking about benchmarking resilience in their financial services industry. So, this is gaining ground as an approach to dealing with critical infrastructures worldwide.

Let me move on to recommendation number two, which has to do with alignment. One of the things we talked about earlier is the fact that no one owns the whole problem. That being the case, we have to figure out how to get the top level guidance such that you drive actions at all levels.

And here, we simply will point out what we perceive to be a bit of a disconnect. I realize this is perhaps overstepping in pointing out a disconnect in Presidential Directives, but we, nonetheless, did so.

If you look at Presidential Direct 7, which focuses specifically on critical infrastructures, you will see that its purpose is to focus on protection against terrorist attacks. In contrast, Presidential Direct 8, which focuses on preparedness, is far more broad. It focuses on all hazards preparedness, but it also focuses on the ability to prevent, as well as to respond.

Our argument is that these two are not driving actions that are well aligned. The National Infrastructure Protection Plan, which is responsive to HSPD-7, is focusing on a subset of the overall issue.

I would also point out that we have seen, in fairly recent events, ample evidence that our critical infrastructures are absolutely crucial to a response to any kind of disaster. So, to not have the critical infrastructure planning deal with the same of holistic of potential threats as our preparedness programs seems out of line.

So, our focus here is that we need to synchronize the top level guidance and make sure that all of the planning is being done with the same context.

We did observe that the 2SR Review that has put infrastructure protection as a key component to the new preparedness directorate gives the opportunity to drive this kind of thinking, and we think that is a very, very positive step. But until we have that kind of alignment, we don't believe that we will achieve the results that are needed.

Recommendation three again will argue for not just the top level goal, but actually, a set of cascading goals that stems from the top level critical infrastructure resilience objective. One of the first things we did was step back and take a look at how this would relate to the National Preparedness Goal, which was a requirement of HSPD-8, and we observed that the preparedness goal focuses on delivering or building and sustaining target levels of capability in particular areas.

And there is a target capabilities list of 36 different items. We observed that critical infrastructure protection is one of those capabilities. So there is, again, the opportunity to begin bringing these together.

The concern we would register though is that while it is listed as a standalone, one of the 36 essential capabilities, we observed that it is also fundamental to most of the other 35. In other words, you cannot succeed in many of those other capabilities without resilient critical infrastructures. So somehow, we have to bring together this interdependency into the planning process to drive the change that we are seeking.

We also realize this is a bit unfair because this is the interim national preparedness goal, it is a work in progress, and I know that there is a lot of ongoing effort in this regard. So, our bottom line recommendation in terms of a goal is that the national goal articulated in PDD 63 puts forth a framework. We would modify it though by extending from protection against intentional acts to building resilience against all hazards. We think those are very, very important modifications.

Secondarily, we would establish that as a top level goal with a framework that cascades down to deal with the individual perspectives of the various stakeholders. We see the need for interlocking goals in order to align the actions, otherwise, we will not effectively address the interdependencies that exist.

Our fourth recommendation has to do with institutionalizing the planning process. We observed over the last couple of decades that the policy and strategic guidance has waxed and waned and shifted in focus based on events. The terrorist attacks caused us to think about physical protection, Y2K caused us to think about cyber and so forth.

We would argue that a far more proactive approach is needed because the threat picture will continue to evolve over the coming decades inevitably. We also would observe that this is a very, very complicated issue for our nation and will require unprecedented cooperation between the public and the private sectors.

I think we will not get it right the first time. So, we would recommend programs that cause us to learn and to think and to evolve the policy and strategy. I was pleased to hear Dr. Thomas observe that resilience, whether it is the resilience of the people or the resilience of the infrastructures, is a deterrent. I believe that as well. I think it is a very strong deterrent. We would offer two specific actions in this regard. One is an exercise program focusing very specifically on critical infrastructures, and here I am not talking about a huge exercise. I am talking about a series of tabletop events that bring together the disparate stakeholder communities. Not only the private sector owners and operators, but also, the communities to whom they deliver services to gain that dialog and understanding. Not on a sector-by-sector basis, but on a geographic or regional basis to understand the implications of these infrastructures and the interdependencies.

We would also recommend an institutionalized lessons learned program not just from the exercises, but also from accidents, natural disasters and so forth. And I know that there are lessons learned activities underway.

For example, looking at the aftermath of Hurricane Katrina. If there is not already a program in place, we would strongly recommend that someone be charged to look at Katrina with an eye toward infrastructure implications.

And I am talking not just the local implications, but what were the ramifications of the loss of the port facilities in terms of Kansas wheat farmers not having shipping access. What were the implications of the disruption in the refineries and the pipelines in terms of fuel shortages here on the East Coast? So, it is that kind of extended or ripple effect that we think ought to be teased out in terms of lessons learned.

I will move on to recommendation five. This has to do again with looking at the diversity between the various sectors, and I realize this is a very challenging area. We also would observe that the definition of critical infrastructures has evolved over the past decade. The list has grown. Sectors have been added that have perhaps less cohesion into the sector than the prior list. The diversity has grown fundamentally. Different sectors live in different regulatory environments. Different sectors have different interdependencies. Different sectors have different stakeholders, and we see the need for a governance structure that acknowledges -- first identifies and then protects the equities of the stakeholders of each of the sectors.

And we realize that there is a need to simply and standardize approaches, but we have some concerns that the approaches currently underway aren't effectively addressing the diversities that do exist.

We also have some concerns that some of the planning approaches have not effective engaged, for example, the state and local governments to whom services are provided. And it is interesting that they are stakeholders not only in the delivery of the services, but they also make decisions that drive either potential resilience or increased vulnerability, in a sense.

One of the most stark examples that can be seen is the consolidation or geographic co-location of right of ways for various kinds of networked communications and services, and the sort of competing desires to consolidate into a fairly narrow area in terms of allocating right of way versus having a greater spread, which increases resilience from a target perspective.

So, we think it is very important for those conversations to begin to occur in a strategic planning sense. And I think understanding and appreciating what can happen in that regard is very helpful.

I would offer in that the White Paper that is provided in Appendix D. It has some very interesting analysis of what can occur.

Our final recommendation I am not going to belabor. We have had many, many studies; many reports that focused on the issue of information sharing. Here we would simply observe that to create an effective policy and information sharing regime it is important to understand what information needs to be shared with whom and for what purpose.
We would also argue though the important thing here is collaboration. This is not about dissemination of information as much as it is about making sure that the right parties are working together cooperatively. I think that is inherently different than some of the other issues.

We would also only observe that many of the, sort of, end users, the people on the receiving end of the information, wear multiple hats. So, there primary hat doesn't read critical infrastructure, and I think that is an important point when you begin looking at the need for an enterprise-wide approach to information sharing systems and processes.

In conclusion, we tried to step back and take a look at where we are today. Many would argue that our critical infrastructures, defined broadly, perhaps are the most efficient in the world. Unfortunately, many of our infrastructures are also aging. They have little, if any, excess capacity and they also tend to be geographically concentrated in many cases and, as a result, are potentially complex amplifying.

By that I mean they are so interdependent that a disruption on one can cause failure to another's. I think recent events have demonstrated that.

There are opportunities to apply technology. Many opportunities. There are ways to upgrade obsolete equipment. There are ways to instrument infrastructures to detect impending failures. There are ways to use modeling and simulation tools to help better understand interdependencies, and also, to look at various trades that could be made. All of that is available.

That said, we think that the only way to move this program forward is to define a shared objective that will cause an alignment of actions across very, very diverse and disparate stakeholder communities. This is what wraps us back around to a very strong belief that resilience is that shared objective and that using that as the heart of the policy and planning guidance will begin to achieve the alignment of action that is needed to move us forward.

I would like to end with a few acknowledgments of people who contributed greatly, either by hosting meetings of the committee or -- Mayor McCrory, we thank you for the wonderful accommodations in Charlotte. The folks at the Naval Postgraduate School and Steve Malphrus, from the Federal Reserve Bank.

I would also like to thank people who contributed appendices to the report. We have simply provided those as additional information to the department; as illustrative examples of some ongoing work that we think is highly relevant.

And finally, I would like to thank Herb Kelleher who took his personal time and corporate resources to share insights. Joe Grano did the same with me, and also, folks from Lucent Technologies, who were very generous with their time and insights. Thank you.

**CHAIRMAN WEBSTER:** Thank you very much, Dr. David. I will ask Secretary Jackson if he has anything that he would like to comment on before we move on.

**DEPUTY SECRETARY JACKSON:** I will take just a quick moment to say that I am very much intrigued by and supportive of the idea of focusing on resilience and thinking about how that effects the way that we structure our work. We have been engaged in a little bit of vocabulary soup as DHS merges, and we have really those four terms: Protect, prevent, respond and recovery.

To some degree or another, the resilience is wrapped around all four of those. I'm a simple Texan. I call that "fixin' to" and "fixin' it". "Fixin' to" is somebody is fixing to do something bad, and we want to make sure it doesn't happen. "Fixin' it," it happened. So we have got to recover and be resilient and quick and nimble about the network.
In the construction of our new preparedness directorate we are really trying to use that word "preparedness" to subsume that totality of the experience from the designing methods to protect, prevent and create resiliency in the networks. And then, that process of how do we align ourselves to act when something bad happens, which is, of course, oftentimes principally a private sector action rather than a federal action. But a federal supporting action is often required and essential.

So, I find a lot to think about in that, and I will take that back to our colleagues to talk about it. As you flowed down through the other recommendation tools about sharing, these other recommendations I think are very valuable. Whether it is information sharing, whether it is trying to create structures to align our focus on resiliency with corporate and other public sector partners, I think that is a valuable thought for us to chew on.

So, I just want to say thanks very much. It is a distinguished group of folks that batted this one around and I think added value for us. So, Ruth, thanks very much for the work.

**DR. COHON:** Judge, do we have time for one quick question?

**CHAIRMAN WEBSTER:** Just about a minute or two.

**DR. COHON:** All right. That is all it will take. A quick observation and then a quick question. Your work is great. Definition is really useful. It has got two components. One is maintaining structure and function. The other is graceful failure. I think we almost never talk about graceful failure.

Furthermore, I think the private sector has very little incentive in terms of marketing mechanisms to deal with graceful failure. Structure and function? Yes. But not graceful failure. There is a lot to be said about that Question. Cyber is crucial to all of these infrastructure systems. I have a sense that the cyber security part of DHS is sort of kind of dropped down in terms of priority for the department. Did your task force look at that? Do you have an opinion?

**DR. DAVID:** Yes. Actually, thank you for reminding me. This was a point that is in the report that I failed to emphasize and should have.

When you start thinking about interdependencies, the very first one to fix is the interdependency between physical and cyber. The two coexist. You have to address the two together. We don't believe that you can separate them; have two separate plans. In fact, one of our observations is that in the front matter for the strategy on securing cyberspace it articulates a list of physical assets that are key to cyberspace. So I think it simply points out that you have to deal with that interdependency first and foremost and then all of the other interdependencies as well.

**CHAIRMAN WEBSTER:** Thank you both. Now, we are ready to start the report on the work of the State and Local Senior Advisory Committee which is chaired by Governor Mitt Romney.

**GOVERNOR ROMNEY:** I'm happy to join you Mr. Chairman.

**CHAIRMAN WEBSTER:** Very good. The floor is yours, sir.

***State and Local***
***by Governor Mitt Romney***

**GOVERNOR ROMNEY:** Thank you so much. First let me explain, on behalf of our entire subcommittee, our appreciation for the fact that the White House and the Department of Homeland Security and the FBI, as well as a number of other federal agencies are using the HSAC and the Department of Justice Fusion Center guidelines as foundational documents. A lot of work was spent putting those together, and I appreciate the fact that they are being used.

Also, the work of our subcommittees on intelligence, as well as information sharing. Those are likewise being used. Of course, as a member of these task forces I appreciate the many hours that have been put in by the members of the state, local, tribal and private sector communities, as well as our federal partners. And the fact that the recommendations are being considered, read and being made part of foundational documents is something which we very much appreciate.

Secondly, with regards to reporting on our most recent meeting, we did come together for a briefing and discussion in early December. One area of focus was to try to understand the roles played by the federal and state and local entities during Hurricanes Katrina and Rita and to discuss some of the lessons learned.

This afternoon you are going to receive the same presentation which we did from the Harris County Texas Judge Robert Eckels. It is an excellent piece of work, and I am sure you will enjoy it. What will come from it will be a number of conclusions, and we had a lot of questions and suggestions.

But one was certainly that a successful response to a catastrophic situation was highly dependent upon prior integration planning and training work. If there has not been that kind of work prior to the occurrence of the event, obviously the response is nowhere near as effect.

Judge Eckels will be showing in his work that on-the-ground management planning worked well, partly because the federal, state and local agencies had planned and worked together before the catastrophe occurred. That is, of course, one of the key take-aways, that the silos that have long existed separating federal, state and local governments and agencies within their respective levels really don't work well when dealing with a catastrophe, and he will have some interesting lessons learned there.

We also received a briefing on federal pandemic planning, and obviously the states and urban communities are addressing this concern. We appreciate the continuing flow of information we are receiving from Health and Human Services and other agencies and the joint planning activities which are underway between federal, state and local governments. I believe that if we can continue to work together effectively on this, that we can be able to respond to a possible pandemic in a more humane and effective manner.

We also spent some time receiving an update from the new program manager's office at the Director of National Intelligence. The bottom line on that is that we are encouraged by the work that they are doing. But there was a sense on the part of our committee members that Washington agencies are encouraging the program manager, the Director of National Intelligence, to go back and rethink and to strategize and to form task forces and to analyze. And the response of our committee was we have had enough task forces, we have had enough analysis, and we have had enough recommendations. It is time to start putting together actions and taking steps and organizing communications vehicles and making sure that we don't allow perfection to become the enemy of progress.

We have spoken time and time again, we have formed task forces, we have talked about the need for a single conduit of information flowing back and forth between Washington, as well as state, local and tribal entities; the need to have information declassified as it flows back and forth.

The new program manger came in and described to us that they were going to form a task force to look at how to share information, and we said, whoa, we have been there. We have been there for a couple of years now. Please use what we have recommended. Don't start over again. Let's see if we can't get something in place first and improve upon it later. So, for those agencies that are making the communication and the direction of the Director of National Intelligence we hope that they focus on taking action and making progress first and then reaching perfection second.

Let me also note, on a separate topic, that as a member of the Critical Infrastructure Task Force I was very pleased with the report. I enjoyed seeing the work. I thought it was excellent because I do believe it highlights one more area where the private sector is ahead of us at the state government levels at least and perhaps other levels of government as well, and that is in the area of resiliency.

And I think we in government have to look to the private sector as a model here. You know, protection is where we tend to focus in government, but it is very, very clear that protection is not enough and that in a world where there is imperfect intelligence sharing, we have to look at the ability of critical infrastructure, particularly cyber infrastructure, to sustain damage and quickly be restored.

I do believe that the HSPD-8 process will be useful in this effort. It is a key issue for DHS to insure that all of our states are using measures of resiliency and to insure that we are able to push forward with this planning. I know the results are going to be incomplete, but we really need to have our feet held to the fire on this.

In my own state we pulled together all of our cabinet secretaries and said we want to have continuity of services and continuity of operations plans for all of the agencies. We divided which things are critical and non-critical and, let me tell you, we have a long way to go. We are putting plans in place, but the fact that we didn't have these off the shelf is an indication that we spent a lot of time on protection, but nowhere near as much time on resiliency and continuity of services.

Finally, as a closing comment I would just like to express a personal delight at the fact that the President and the Secretary have chosen George Foresman as the new Under Secretary of Preparedness. We got a chance to work with George Foresman on a number of our task forces. He is a brilliant person with extraordinary expertise.

I am also delighted that we are seeing at the highest levels in our domestic preparedness someone who comes from the state and local world. Over time the tendency has been to grab people who have federal experience, military and otherwise, and that is as it should be. But, boy, it is really encouraging to see someone with a state background, as he comes from the State of Virginia and worked with two administrations there. To see him coming in and playing a very senior role is something that we are very pleased to see as a task force. So, with that, Mr. Chairman, I conclude my report.

**CHAIRMAN WEBSTER:** Thank you very much, Governor. I just want to interject how pleased I was to hear your emphasis on the importance of prior integration and training. I know from my own experience in heading the review of the riots in Los Angeles in 1992, following the Rodney King verdict, that this lack of integration, prior integration and training, was the single most cause of the scope and extent of the damage.
I also agree with your realistic emphasis on the importance of resilience, because in an imperfect world we cannot rule out the catastrophic events that we should be prepared to deal with. Mr. Secretary, would you like to say anything?

**DEPUTY SECRETARY JACKSON:** A very, very quick one. Governor Romney, thank you for your work and thank you for your kind remarks about George Foresman. We are trying to intrude the real world into DHS. Sometimes that is a force feeding process, but I know that having a new colleague with this background a great benefit to us.And I will take as a homework assignment to make sure that you know and that we act upon this issue you have raised about not reinventing the wheel on the communications tools that we need to work more closely with our state and local colleagues. We are not going to set a whole series of groups out into the world to take a look again at the work that you have already done on fusion centers. We will leverage that instead to try to make progress faster.
So, there is a good bit of things that have been delivered that we can work with, and we will take those and use them quickly. And we will do very collegiately with program mangers as well.

**GOVERNOR ROMNEY:** Thank you, Secretary Jackson. That is very encouraging.

**CHAIRMAN WEBSTER:** Thank you for being with us, Governor.

Now, we are right on schedule, and our next and last task force report is on private sector information sharing, which is chaired by Mayor Pat McCrory and his Vice Chair, Herb Kelleher.

***Private Sector Information Sharing***
***by Mayor Patrick McCrory***

**MAYOR McCRORY**: Thank you very much. Let me first apologize for my voice. I am hoarse because I was at the New York Giants game playing the Carolina Panthers in New York, and I lost my voice cheering on the Carolina Panthers to victory. I want to let the Governor know that we look forward to playing New England in the Superbowl in Detroit, Michigan.

Let me also say that I think it is a good transfer from Governor Romney's report to our reporting, talking about the private sector and integration, and we have long known that 80 percent of the infrastructure is actually owned by the private sector. I don't think that most government officials and most media people and most of our public quite understand that, because it seems to be that the entire burden of information and response seems to be put on the federal, state or local government when, in fact, the private sector is going to play the most important role.

We have seen this through the Katrina issue. Frankly, to recover from Katrina, to recover from any disaster, whether it be a natural disaster or a manmade disaster, we realize that the quicker you get the power on, the quicker you have the private sector get the cell towers or the telephone lines prepared, the quicker we get the gas supply corrected, as we saw that up and down the west and east coast, the quicker we get the airlines to help in the evacuation, the better prepared we are going to be in responding to either type of disaster.

I think Katrina is actually a good role model in understanding the importance of the private sector and how -- by the way, Herb, your airlines and many others were an integral part of that response and continue to be. That is really the emphasis of what our committee worked on.

I would like to thank Candy Stoltz and I would like to thank my Vice Chairman, Herb Kelleher, for really understanding and emphasizing the need for the private sector to be the major part of a response and also of the prevention, and I think it compliments the other two major reports that we got earlier this day.

What we learned in our committee, and we have already submitted our report and I am not going to repeat the report, is this: We have to have a communication line and a trust level between the private sector and the government entities.

We outlined very detailed in this report, Mr. Secretary, that currently there are laws that prohibit the Herb Kelleher's of the world from getting necessary information from the government which will help protect his airline. Getting information to the power companies, getting information to the chemical companies and other parts of our industry that must have this information.

We have very specific information and recommendations in this report which say we have to change the laws which allow you to share that information with the private sector, and on the other side of the specter we have got to have more impetus put to allow the private sector to share more information with you.

Right now we are failing on both ends because, as we have stated in our report, and it is detailed and outlined, there is a strong reluctance of the private sector to share security information with the government for fear of what is done with that information, what the media may do with information and where their customers may respond to that information.

We have very specific recommendations in this report in setting up third party entities which would be a conduit between the government and the private sector in sharing that information, and I think those are the two most important parts of this report, the sharing and the trust between the private and the public sector.

If we have that trust, if we have the laws that allow us to do that, I think you are going to see, first of all, prevention of potential disaster from terrorists, and also, a better response in natural disasters in the areas of getting the power turned back on, the cell towers recovered, the gas supplies corrected and transportation in place. And therefore, we will then save lives.

We have not gotten a response yet from this report. We look forward to that response. There are a lot of details in there that we have already given, and I am not going to repeat that.

We do think there is also important information in which, if requests are being made of the private sector, first confer with the private sector before those requests are being made so that trust can be established and very well understood.

With that, I would be glad to have my very distinguished Vice Chairman of the committee -- if you would like to say anything else to compliment my remarks or disagree with my remarks?

**MR. KELLEHER:** No, Mayor. I would like to say something that I don't think will offend you, and that is that I have served under a billion charismatic and highly intelligent leaders with respect to the information sharing task force, and I was inspired throughout by your leadership.

**MAYOR McCRORY:** The payment has already been made underneath the table from the private sector to this Mayor.

**MR. KELLEHER**: I thought you were still running.

**MAYOR McCRORY:** The election is over, Herb. But again, I would like to thank your staff who has done an excellent job in working with us, Mr. Secretary. But we do need to move quickly, and I think Katrina shows that even more.

**CHAIRMAN WEBSTER:** Thank you very much, Pat. Does any member of the council have any questions or points that they wish to make?

**CHAIRMAN WEBSTER:** All right. Thank you. Well, we remain on schedule. I am going to turn the meeting over now, as we get ready to approach adjournment, to our Executive Director, Dan Ostergaard. Dan, the floor is yours.

***Closing Remarks***
***by Daniel Ostergaard***

**MR. OSTERGAARD:** Thank you, sir. I just want to take a moment to say thank you. Tomorrow will be my last day with the department. I just want to say I haven't gotten here certainly without standing on the shoulders of some real giants.

I would like to point out, if I may, some of my staff. Candy Stoltz is here, Mike Miron, Jeff Gaynor and Michael Fullerton. Carnes Eiserhardt is walking around here somewhere keeping the noise down upstairs. Richard Davis is in the back of the room, formerly with us and now over at the White House. And also, Katie Knapp, who is currently over at the Department of Commerce.

And truly, these folks have done a great deal behind the scenes, and I really can't express my appreciation enough.

Also, I would like to thank all of you, clearly, for your service, especially in a time of crisis in this country. If you look at the threats that face us, it is very real, and I applaud you for your patriotic duty. I think it is inspirational. I certainly appreciate it.

I recognize the fact that you all have other jobs, other things you could be doing, and yet you volunteered to participate in this and you put a lot of long hours in. And I can't thank you enough, both on behalf of your services to the President and certainly your service to the departments, but more importantly I think your service to the nation has proved invaluable. And for that, I truly thank you and am humbled by it. Thank you.

**CHAIRMAN WEBSTER:** Thank you very much, Dan.

**DEPUTY SECRETARY JACKSON:** Can I just say a word on that score?

**CHAIRMAN WEBSTER:** Certainly. Please.

**DEPUTY SECRETARY JACKSON:** I don't want to have the opportunity pass to get a chance to say thanks to Dan. Dan has been a superb colleague, has been part of the founding team of DHS and has helped us shape this tool in a very, very valuable fashion. He is a good guy, and we have benefited very much from his work in this area.

We wish him all of the best. We know we haven't seen the last of him. You have become part of the family, Dan, and you are always welcome at family reunions. And we will call upon you, I am sure routinely, to help us in the future.

So, on behalf of the Secretary, and really, his entire team, please know how much you have been appreciated and how grateful we have been for your great work. I can't quite match the flowery pros of Herb, but why don't I just say "that too."

**MR. OSTERGAARD**: Thank you, sir.

**CHAIRMAN WEBSTER:** Well, I think the applause spoke for how the members of the council feel, Dan. I just wanted to express my personal appreciation to you. You helped us through a change in leadership on the council, and it has been my experience that any requests for information or for action was promptly addressed by Dan.

He represented us well in the department and in a department that is struggling not to lose good ideas and to be responsive to good suggestions that you have done an able and courageous, at times, job under, and I wish you all the success in the future.

**MR. OSTERGAARD:** Thank you, sir.

**CHAIRMAN WEBSTER:** All right. Now we are at a point now when I think it is necessary and advisable for me to advise the public, as I said that I would, that any members of the public who wish to submit comments to the Homeland Security Advisory Council may do so by sending us a letter or on inquiry.

The address is Homeland Security Advisory Council, U.S. Department of Homeland Security, Washington, D.C., zip code 20528. Or, you may fax us at 202-772-9718. Again, 202-772-9718.

Any additional information or copies of the previous minutes of meetings can be found on line at www.dhs.gov/hsac, and the minutes of this meeting will appear on that web page within 90 days.

Thank you very much for your participation, thank you all on the council and all of the members of the public here with us today. We have a job to do, and we intend to do it. The meeting is now adjourned.

**HSAC Meeting Adjourned 11:59 A.M.**