THE BROOKINGS INSTITUTION

THE FUTURE OF HOMELAND SECURITY

Washington, D.C.

Friday, September 5, 2008

Introduction:

MICHAEL E. O'HANLON
Senior Fellow, Foreign Policy

Featured Speaker:

MICHAEL CHERTOFF
U.S. Secretary of Homeland Security

* * * * *

P R O C E E D I N G S

MR. O'HANLON: Good morning, everyone, and thank you for being here. I'm Mike O'Hanlon from Brookings. And on behalf of all of us here, we're delighted to have Secretary Michael Chertoff speaking today in what is one of several mega-strategy speeches he's giving to help reflect on the lessons of his tenure at DHS, where he has been the Secretary for about three and a half of the five and a half years of that department's existence.

We're just thrilled to have him here at Brookings. As you know, he was a federal prosecutor for about a decade, also a judge on the 3rd Circuit Court. He's now been in this position, as mentioned, since February, 2005. Please join me, without further adieu, in giving a warm welcome to Secretary Chertoff.

SECRETARY CHERTOFF: Well, Michael, thank you for that kind introduction. And I want to thank Brookings for inviting me to address you. Also regards to Strobe Talbott, who I know couldn't be here.

It's really wonderful for me to have the opportunity to join you to address some of the long term security issues that are going to be facing our nation over the next five years. As it happens, I come to you in the middle of what's been a very busy two week period. We've just finished the immediate response to Hurricane Gustav down in Louisiana.

We have Tropical Storm Hanna coming up likely – actually, it's going to hit this part of the country in the next couple of days. And, of course, we have Hurricane Ike, currently a category four storm, which is also headed for the United States.

This unusually busy period during hurricane season provides a good backdrop for what I want to talk to you about today, which is our nation's critical infrastructure, the things we rely upon to make it possible for us to go about our daily business.

And in particular, I want to base my remarks this morning on a forward looking view of Homeland Security, where are we vulnerable, particular with respect to our critical infrastructure, what consequences will these vulnerabilities have as we move further into the 21st century, and how can we collectively address these vulnerabilities using 21st century solutions.

Now, to put this in context, this is the fourth in a series of five speeches that I am in the process of delivering this year in the wake of the department's fifth anniversary. In the first speech, I spoke about emerging 21st century threats, both man-made and natural. These include terrorism threats from groups such as al-Qaida and Hezbollah, and because DHS is, in fact, an all hazards agency, I also talked about natural threats, such

as hurricanes, earthquakes, and infectious diseases, which will continue to be serious sources of danger for us in the years to come.

The second speech I delivered covered our prevention strategy, or more specifically, how we work to keep man made threats from harming our citizens. We do this, of course, by keeping dangerous people and dangerous things out of the country, and also by utilizing the hard power of the military overseas and the soft power of diplomacy and foreign aid, all working together to try to curb radicalization, to reduce the threat, and thereby, to reduce our overall risk.

The third and fourth speeches turned from the issue of prevention to the issue of how we harden ourselves when prevention doesn't work, either because we can't totally prevent a threat from coming to fruition, or because we're dealing with a natural disaster which is beyond our control to stop. Last month I spoke in particular about the vulnerabilities associated with the protection of our most important asset, our personal identity, and how we have to work harder than ever to close the increasing vulnerabilities to the protection of our personal identity by using 21st century tools to increase the measure of identify protection we can afford all American citizens.

But today's topic is going to cover a different kind of vulnerability, not the vulnerability to our identity, but the vulnerability to the physical world in which we operate, that is our critical infrastructure.

And I want to particularly talk about how these vulnerabilities look to me as we enter the 21st century and what we have to do to reduce the risk to our critical infrastructure in the years to come.

Let me begin by outlining the fact that I think there are two very different views that are often offered when we address the question of how to reduce the threats and the vulnerabilities in our critical infrastructure. One view is basically a government-centric model. It's a view that takes the position that the federal government really should pull the laboring oar in reducing vulnerabilities to all of our critical infrastructure and protecting the public. Under this view, homeland security is essentially a government function in all respects. And, therefore, Washington should figure out where the vulnerabilities are, should dictate to the private sector what the private sector should do to reduce those vulnerabilities, and in many cases, that the government should simply send its own personnel to guard the most critical vulnerabilities and the most critical infrastructure all across the country.

Under this view, essentially any business which operates or owns critical infrastructure ought to be managed with a great deal of detail

and a great deal of specificity by officials in Washington or in state capitals, that the only way to show we're truly serious about reducing vulnerabilities is to have a lot of regulation, preferably painful or punitive regulation, and that where we see threats that we have to protect against, federal boots on the ground should be involved in guarding those particular elements of infrastructure.

Now, I term this a kind of 20th century command and control view of how you protect things. Some would argue it's really kind of a version of old Soviet style heavy regulation, lots of visible, people in uniforms, lots of very specific mandates from government, all of which are designed to assure that the people who own and operate the infrastructure are protecting it. Of course, it's ironic that many people who argue for this position are also the first to criticize the federal government when efforts to use this kind of command and control approach fall short.

Let me give you a concrete example of what I mean by this 20th century command and control approach. One of the things we're very concerned about, of course, is cargo security, how we make sure people don't put dangerous things in containers that come into the United States.

Some people have the view that the only way to deal with this is literally to send Customs and Border Protection officers overseas, to

demand that they either inspect or at least scan 100 percent of American bound cargo containers before they're loaded onto ships.

Some people think we should physically inspect every one of those 100 percent cargo containers using federal law enforcement officials before they are released into the country.

And the views are if we don't do that, we're being dangerously lax in protecting against this threat. But actually, the approach that we take is not this 20th century command and control approach, it's rather a 21st century partnership approach, which attempts to apply risk based standards to evaluate where the true danger lies with respect to our container supply chain, that involves business input into how to design a system to reduce vulnerability, and that relies upon business to do a great deal of the security checking itself.

And the reason we do that is because it's simply impossible for the federal government, certainly within any reasonable budget, to take on the responsibility of micromanaging the business operations of every major business activity in the United States and to supply federal boots on the ground to all of those businesses to reduce vulnerability.

Our position, rather than the 20th century command and control position, our position is that the 21st century requires a different approach to protecting critical infrastructure, and that's what I call a

partnership approach. It's an approach that is not merely relying on government, or even mainly relying on government, but that looks to work with the private sector to leverage their capabilities and their incentives together with federal government know how to get the maximum reduction in risk for the most efficient use of resources. This 21st century approach to reducing vulnerability is focused on cooperation and stakeholder input. It's based on the recognition that most businesses are very keenly aware of their personal incentive to maintain security and to protect their own assets and employees.

The fact is that the government of the – the federal government or the state government does not need to order people to protect assets when the people themselves place great value on the assets. What we have to do is, we have to help them do the job they have a natural incentive to carry out themselves.

People who run complicated businesses, global businesses, don't need the government telling them, through heavy handed regulation, that if a flood wipes out their computer system, they're going to be out of business, and therefore, they ought to keep their servers in a high enough position to avoid flooding.

In fact, what these businesses do need is information and guidance about the best way they can carry out what they're already

motivated to do, which is to make sure that their investments are secured and that the people who work to carry out their businesses are safe. The partnership model also acknowledges the reality that it's simply impossible and impossibly expensive for the government to handle 100 percent of Homeland Security preparedness, prevention, response, and recovery responsibilities in the 21st century. There are simply too many places, too many things, and too many people for the government to take on the job of doing everything itself.

What the government can do is work with natural self-interest of people and businesses, to help them be most efficient in protecting their own property and their own employees.

Based on this understanding, therefore, our approach using the 21st century partnership model has been to set performance standards and metrics, to give guidance and advice, and then to audit through responsible third parties so that we can be sure that the private companies are, in fact, carrying out what is in their own rationale self-interest.

This approach allows the flexibility for businesses to tailor security measures to their particular business operations. It allows them to use their own intimate knowledge of their own processes to be efficient in protecting their assets and their people. But it also gives us the ability to make sure that we can ultimately judge the success of their efforts, and

if necessary, if those efforts are unsuccessful, to then stand in and perhaps give them what I would call, using a technical term, a little bit of a kick in the pants to make sure they do the job properly.

Let me give you two examples of what I mean by this 21st century approach. The first involves a set of chemical security regulations that we were given the authority to issue by Congress a couple of years ago. Everybody recognized that there was a clear vulnerability with respect to some chemical facilities that are located in high population areas, a vulnerability that could be exploited by terrorists who might attack those facilities and cause a dispersal of the chemical with very, very serious consequences to the surrounding community.

We knew we needed a sensible solution, but we also knew that the option of simply sending boots on the ground to guard every single chemical plant or imposing billions of dollars of cost based on what bureaucrats in Washington believe is the best way to guard each individual plant, we realize that that approach would be prohibitively expensive, it would probably seriously damage the very industry we're trying to protect, and it probably wouldn't do a very good job of reducing vulnerabilities. So what we did is, we worked with Congress, we worked with the industry, we worked with the communities, we worked with

stakeholders, and we worked with academics to look at the entire chemical plant system across the country.

We put together a framework that focused on where the highest risk facilities were, with the most dangerous chemicals and the most vulnerable population centers. We basically tiered the risk. The highest risk were in the top tier, and then as we went down, analyzing the particular vulnerabilities and the particular communities, we had lower risk tiers.

Based upon the degree of risk, we directed companies to achieve certain performance outcomes. They had to complete security vulnerability assessments if they were in a high risk category, and they had to submit them to us, they had to develop site security plans, and they had to implement risk based measures that will meet the standards, the performance standards that we set.

This allowed them to decide the right way and the most cost effective way to achieve the result, but it allowed us to set the standard that's required and the result that must, in fact, be reached. And that's what I mean by a partnership. We set the standards, we set the performance outcomes, but the actual implementation is carried out by the companies that know best. It's like the old saying, there are a lot of ways to skin a cat.

Now, it's not to say that this approach is without teeth. I'm not naïve about the fact that there are always a few companies that somehow either don't appreciate their rationale self-interest in meeting these standards or companies that may feel that if everybody else does the right thing, they can kind of hide in the tall grass and maybe get away on the cheap without doing what they need to do to protect their own assets and to protect the surrounding community.

So we did put a little bit of stick into these regulations. We determined that if companies fail to follow through on the security enhancements, if when they were audited, they hadn't met the performance metrics, then, in fact, we were prepared to levy some pretty tough penalties, including fines of up to $25,000 a day.

The outcome here, and the result of this is, a system that allows the vast majority of responsible companies to find the most efficient way to satisfy security requirements, but gives us the ability to find the irresponsible actors and to punish them, to make sure that they come into line with what the general standard really is. I'll give you one more example of the partnership model which can be found in the safety act.

That act, as you may recall, provides for liability protection for anti-terrorism technology companies. It's designed to give them an

incentive to come up with cutting edge anti-terrorism technology in a way that shields them from unreasonable liability exposure.

With Congress' help, we formalized liability protections and incentives that encourages the technology industry to play a crucial role in developing Homeland Security technology, but also limits the exposure to unnecessary and sometimes counter productive litigation that sometimes bedevils a lot of our efforts to spur technological development that helps the vast majority of people.

Again, it's the recognition that if we unleash the industry and our partners in the private sector, we're going to achieve more positive results than if we try to dictate to them the best way to achieve outcomes. If I stand back and I look at the whole approach that we take, therefore, in this partnership model to infrastructure security, and if I were to give you one kind of bottom line on what I think is the most successful way that we've found to approach this problem, I would look at the way in which we've organized the entire economic – all the economic sectors of our country in order to work again on a partnership basis to identify across the board where our critical assets are, what our most serious vulnerabilities are, and what are the tools that companies can use and that government can use working together to reduce those vulnerabilities.

In the last couple of years, we've implemented a national infrastructure protection plan. That is a collaborative strategy involving federal, state, and local tribal and private actors, designed to identify all the areas of critical infrastructure, the most important assets, the strategies to protect those. It's designed to give us the ability to have visibility into what companies are doing. It gives us the ability to give those companies information that allows them to modify their plans, and it does it, again, in a way that allows for real flexibility.

We've created 18 sector specific plans ranging from information technology, to energy, to dams, and most recently, to auto makers, heavy equipment manufacturers, and steel producers, recognizing that there can't be a one size fit all program for how to protect our infrastructure, that what you need to protect dams is different from what you need to protect IT systems, that what you need to do with respect to our energy infrastructure is different from what you need to do with respect to our commercial establishments.

And by working with each of these sector counsels, we have a natural point of contact for interactive development of a series of plans that gets the best ideas from private industry and the information and intelligence that we can provide from government to provide the maximum

benefit in the most efficient way for protecting each of these important sectors of the economy.

As part of this, we put together a comprehensive list of almost 3,000 national assets, systems, and networks across all of those 18 critical sectors. Let me tell you what this means; it means when there's a hurricane in the Gulf, or some kind of a series of fires out west, one of the first things I am able to see is, what is the critical infrastructure in that part of the country that is of national concern or regional concern. That allows us to know exactly what we have to move to protect, what we have to move to restore as quickly as possible, what we have to be able to work around while a particular piece of infrastructure may be out of action, and that visibility and that ability to go directly to those economic actors and business actors has time and again – hasn't eliminated the pain of some of these disasters, but it has reduced the pain of disasters that otherwise might have a much more serious cascading effect across our country, with health consequences, with consequences in terms of peoples individual safety and security, and with serious economic consequences.

Not only are we doing this focus survey on our vulnerabilities and our critical infrastructure here in the U.S., but we are actually doing it overseas, as well. Through our critical foreign dependencies initiative, a new initiative we launched last year, we have now looked overseas at a

number of countries and identified those elements of critical infrastructure in other countries which have very serious consequences for us, so that we know, for example, if a particular refinery went down somewhere else in the world, that would have an impact on our energy situation. So we know that if, for example, a particular natural gas field in another part of the world were impacted, that would have a consequence for our infrastructure, by identifying and focusing on assets in systems that are located abroad on which we, as Americans, are dependent, we can do two things.

First of all, we can plan for the possibility of disruption if there should be a disruption in that foreign critical infrastructure; and second, we can work with our foreign partners and with foreign companies so that they can put into place the measures to protect their infrastructure, which is of benefit to them and benefit to us.

And it would surprise you to know, I'm not going to necessarily get into the specifics here, that we are currently working in different parts of the world with other governments, helping them secure critical assets that are of importance to their citizens, as well as to our citizens.

But as much as I've talked about partnership with the private sector and the need to make sure that we guide the private sector, but not in a way that's too heavy handed, I also want to be candid and say there

are some times when government does have to play a greater role in protecting our critical infrastructure. Again, this is not in the area where there's a one size fits all, or where there's a particular cookie cutter approach we can take. And basically I'm thinking in particular of two areas where I think government has a much larger responsibility to play a role in protecting our infrastructure and assets than might be the case in a normal business context.

The first are those instances where we're dealing with what I call common goods that are publicly owned. The kind of critical infrastructure that is under public ownership and public supervision, that doesn't serve the interest of a particular business, but rather serves a wider community interest. What do I mean? I mean things like our bridges, our highways, our levies which protect whole communities, which are owned and operated by the government.

Obviously, in these cases, the government has to take full responsibility for making sure that we are adequately protecting that infrastructure.

A secondary area involves infrastructure that is in private hands, but which is critical to other businesses and critical to a large part of the population in terms of the consequences of failure. For example, private businesses dealing with energy transmission have responsibility

not only to make sure – from a business standpoint, not only to make sure they're protecting their own assets and their own employees, but they have to recognize that their failure will have a major cascading effect that will touch hundreds or thousands of businesses and possibly millions of people, and in that instance, the government has to play a greater role to recognize that the – because the consequences of failure are so great, and because the cascading effects of failure are so wide, government has to make sure that private businesses do take on the responsibility that is commensurate with having such a critical role in an interdependent economy.

Now, I have to be honest, we've made a lot of progress in terms of these common goods, publicly owned and privately owned, when it comes to protecting them against possible terrorist attacks, and a lot of that has been through the process I've described including our national asset data base which is designed to focus on national assets that are vulnerable to terrorists.

But regrettably, I don't think we've done quite as good a job in protecting our common good assets and common good critical infrastructure against simple wear and tear or threats from Mother Nature. I've seen a similar pattern time and again. When it comes to making long term investments simply to maintain the things we rely upon against the

normal passage of time or against the kinds of natural disasters that are eminently predictable over a long period of time, we have failed time and again to devote the energy and the effort and the investment to make sure that these structures can be preserved in the face of a possible very serious natural disaster, or frankly, simply through the ordinary degradation of any physical structure that comes year in and year out.

We've seen sometimes that because of resistance to spending money on long term investments, we haven't put enough in our levies, dams, and power grids. Of course, when a disaster occurs and these systems fail, then we have to turn around and pour huge amounts of money into emergency relief, response, and recovery, and rebuilding, often much more than we would have had to spend if we had had a disciplined program of putting the investment in over a long period of time.

In fact, I sometimes describe this as a kind of musical chairs when it comes to protecting our infrastructure against natural disasters. Since we don't know when the disaster is going to occur, office holders and politicians sometimes take the position that they're hoping that the music doesn't stop and the disaster occurs until they're out of office. And that, of course, leads to a very – it's kind of playing Russian roulette with our citizens' safety.

Let me give you some concrete examples of the kinds of challenges we have in dealing with protecting against natural disasters for these major common goods in the face of some of the competing political forces that operate in the real world.

First, let me take you to the Sacramento Levy System. Of course, we're focused on levies in New Orleans, but some of you may know that Sacramento, California has a very significant levy system, and is, in fact, one of the top at risk urban areas in the country for flooding, having experienced five record floods in the period of just 46 years, from 1951 to 1997.

A major catastrophic failure of levies in Sacramento would not only have serious impact on the population, but could potentially effect the watershed for a good deal of California. And imagine a large part of California with water that became unusable for drinking and for agriculture. That would truly be an apocalyptic catastrophe. And yet for decades this area of Sacramento has been protected by a patchwork system of aging levies that were built 100 years ago, when all there was was a little bit of farm land, and therefore, what was at risk was considerably less than what is at risk today.

These levies are made out of, in many cases, out of earth, and they're designed basically to fail at a certain level, when the water

floods a field, and then you rebuild the levy. But because of a tremendous amount of heightened development, homes built, and I've seen this myself, literally in the shadow of these levies, what is now at stake if a levy fails is human life, human safety, economic development, and a good deal more.

The fact is, in Sacramento, we have a dangerous situation, where a heightened risk of flooding, poor levy maintenance, and very rapid development, without serious and adequate building codes, have all pointed and created a recipe for disaster.

Now, a couple of years ago I was out with Governor Schwarzenegger, and he has been very vociferous in leading the way, working with FEMA and the Corps of Engineers, and with State of California and local emergency agencies to do everything possible to address the situation. Some of that involves emergency planning, but some of it also involves putting the effort into rebuilding and securing these levies. In February, 2006, the Governor declared a state of emergency and authorized immediate repair work, which was followed by a voter approved $4 billion bond plan to fund levy repairs and flood control projects. These are exactly the right thing to do, major steps forward.

Additionally, beginning in 2007, we partnered with California to conduct a comprehensive review of the California state water system.

And we have also worked with the Army Corps of Engineers to come up with maps that adequately warn people about where the flood plains are so that appropriate building code restrictions on development can be put into place.

This is all well and good, but what was the reaction? The reaction to this was vigorous and angry push back by some local development officials and businesses. In recent articles in the *Sacramento Bee* and other papers, underscore how local county officials and local officials have complained about new flood maps, have complained about the requirement of elevations in flood zones, because they're afraid it's going to effect development, because they're afraid it's going to effect jobs, because they're afraid there's going to be a moratorium on building while these new levies are constructed. And it is confronting this kind of push back, based on peoples desire for immediate economic benefits, based on peoples desire for immediate gratification, that puts the population of these highly developed areas at great risk and raises the danger that if we were facing a levy collapse, the consequences might be much graver than if we put into effect those measures which prudence tells us we ought to engage in in order to reduce the risk of flooding.

Let me give you another example, New Orleans itself. We all remember in 2005, that the true impact, the true impetus for the major damage to the city of New Orleans itself was the failure of a levy wall on the 17th Street canal.

And to get very specific about what happened, as the water in Lake Pontchartrain began to rush back after the hurricane to the southern bank, it put an enormous amount of pressure on the canal that goes right through the city of New Orleans at 17th Street. The canal operated almost as a funnel. The water was surged into the canal, there was enormous hydraulic pressure, and the walls failed. And because of that failure, a good deal of the city of New Orleans filled up like a bathtub. Now, there's no question that there were structural problems with the way that wall was built. But when I was out in New Orleans about a week ago and I went to the 17th Street canal so I could put my own eyes on the canal and satisfy myself that it was less vulnerable than three years ago, I saw that there was a giant barrier in place right at the point at which the canal meets the lake.

That barrier, which is basically raised day in and day out, allows the Army Corps of Engineers, if there is a rise in lake level and a surge, to drop a massive steel gate that would prevent that water from entering the canal. That would have the effect of preventing the kind of hydraulic

pressure which caused the collapse of the 17th Street wall three years ago.

So I asked the question, I said, you know, this seems like a pretty obvious thing to do, why wasn't this done ten years ago, because if it had been done ten years ago, then when Hurricane Katrina came, they would have dropped the gate, there would not have been a surge into the canal, the canal wall would not have failed, and the city wouldn't have filled up, and an enormous amount of loss of live, heartache, and economic damage would have been avoided. And, you know, I was surprised to find out that actually ten years ago, the Army Corps of Engineers proposed putting just such a gate up at the 17th Street canal, a gate that had it existed in 2005, would have prevented a good deal of the damage to New Orleans.

What happened? Well, the BBC went back and did a study of all of this, and here's what they said. The Army Corps first proposed putting these gates into place nearly ten years ago, but the idea did not get off the drawing board as it was opposed by local residents who thought it would spoil their view of the lake, and environmental groups concerned about its effect on the ecology of the area.

I want you to think about that when you have in your mind the vision of what happened to those residents of the lake and the ecology when the water surged into the canal and the levy broke.

Now, not only are we talking about, as I said, publicly owned common goods, we also have to look at the same problem that arises with private businesses when they happen to be pivotally located in a way that everybody else in the community depends on it. And the great example, here again, taken from just last week, is the issue of power. After a disaster, you can't get power up; if you can't get power up, you can't get food to people, you can't get people to safety, you can't begin to rebuild businesses. Everything depends on the ability to move energy as quickly as possible into an effected area.

That means the transmission lines through which everything surges become critical in responding after a hurricane or a natural disaster hits. It also means that when we have gasoline stations on which everybody relies so they can fill their car up so they can go to the grocery store and get goods, when those gasoline stations can't pump because they don't have their own energy, then everybody else is stalled in the effort to recover. We saw this in 2005 with Hurricane Rita and with Hurricane Wilma.

So in 2005, we said to the oil companies, Secretary Bodman and I wrote a letter in which we said, look, you ought to give your gas stations generators, because when a gas station goes out of business because the power grid goes down, it's just – more is at stake here than just the revenue for the gas station owner or the revenue for the oil company. What's at stake is the ability of the entire community to start itself up again, for people to be able to feed themselves and have decent comfort and decent amenities. Therefore, because of the amount of reliance the community places on your gas stations, you have a greater perhaps than average responsibility to make sure those gas stations can get up and running as soon as possible.

Unfortunately what we saw was, there was a very uneven response to this requirement. The state of Florida actually passed a law requiring gas stations to have generators, precisely because they recognize that the consequences of gasoline station failure were much greater than the consequences to an individual company.

But many states haven't done that, and many companies haven't responded responsibly to the request that we made to outfit their retail outlets with the necessary capability to get up and running as quickly as possible.

What all of these things have in common is, the fact that we are dealing with infrastructure that has enormous consequence for people that goes well beyond the individual business owner. And in these cases, we have an obligation on the part of the government to see to it that people live up to that broader responsibility. And at the same time, we cannot allow ourselves to get side tracked by the typical push back from economic interest or aesthetic interest or environmental interest that seek to stop every major project because parochial concerns will inevitably be stepped on or overridden for the greater good. It's really about putting the common good first when it comes to the issue of our critical infrastructure.

So what is my proposal? Well, my proposal is, first of all, to recognize that there's no single, again, no single cookie cutter approach to this issue of vulnerable and crumbling infrastructure, but that we do have some models we can look to as a way to guide us in how we deal with addressing our infrastructure vulnerabilities, not just from terrorism, but from natural disaster and wear and tear over the years to come.

First, I'd begin by saying we have to have a risk based approach. We should build on the model that we used with respect to terrorist threats and broaden it to begin the process of identify critical infrastructure that we have to worry about from the standpoint of natural disasters and simple wear and tear. This is not just, by the way, a federal

government responsibility, it is a responsibility that the states and localities also ought to undertake. From the federal standpoint, if we looked at the top 500 to 1,000 high consequence, high risk assets, we could begin the process of planning how we drive down and reduce the vulnerability for those assets. If every state took on that responsibility for purposes of establishing its own baseline of critical infrastructure, we would soon have a network across the country where government had a clear picture of what it is we have to maintain and protect in order to make sure this country is well situated to function even if we have some kind of a natural emergency.

Once we've identified this infrastructure, we have to have a real strategy about how to make sure we maintain and protect it. Now, this involves making some tough decisions and asking some tough questions. We need to evaluate how much money it's going to take over the life of these projects to maintain and, if necessary, reinforce them against the degradation that would occur if there were a disaster.

We have to consider how much long term maintenance is going to cost. And we have to also evaluate whether it's cost effective in some circumstances to allow building in certain areas where the necessity to protect that built up area will require such a costly investment that it may simply not be effective. In other words, it may make more sense to

say you can't build here because the cost of protecting the area far outweighs the benefit to a small number of people who are seeking to develop a particular area.

This is much easier said than done, because it requires the discipline to withstand some very powerful and very deeply committed interest who will be interested in developing in those areas, or who will have other uses for the money that will be spend on not particularly glamorous things, like bridge repair, or levy repair.

But if we don't do this kind of a strategy, what we will find again and again is that we are frittering our budget away on perhaps things that have a short term benefit or things that may have a short term popularity, but that when the actual crunch comes, we will not be able to say that we have done what we should do to protect those vital elements of our national infrastructure on which we all rely.

Finally, once we develop this strategy, we have to have an ability to follow through on the commitment. You know, I have seen in the almost four years I've been in the job, often we begin projects with a great deal of hoopla and a great deal of enthusiasm and a great deal of public support, but with the passage of time, as the telephone lights get turned off and the news turns on to a different topic, the degree of commitment

begins to wane, and all of a sudden, other things on which money could be spent begin to be more popular and more attractive.

The difficulty with the kind of long term infrastructure protection program I'm talking about is, it's not going to be done in a week, or a month, or a year, it's not going to be done during the period of time that we begin the project with enthusiasm, it's going to require the commitment to follow through over a period of five years, ten years, 20 years, but if we don't do it, we're going to get back to that old game of musical chairs, where we simply hope that the music doesn't stop while we're in office, and then that poor, unlucky guy who is in office when the music stops is going to find himself without a chair and falling to the ground. That is simply not a responsible way to protect our country and the next generations.

The one thing we know is this, our critical infrastructure is going to outlast the term of office for most of the people in government today, it's going to outlast the politics that go in year in and year out, and it's going to outlast the kinds of funding conflicts that we typically deal with in each budget cycle. Therefore, the process of identifying the critical assets, coming up with a serious maintenance strategy, and committing to carrying that out has got to be a multi year concerted effort.

We have begun to do this in the area of counterterrorism with the national asset data base and the kinds of investments we have made in counter terrorism activity during the last five years.

What I'm now urging is, we take that same disciplined approached, based on partnership, based, when necessary, on strong government action, based on clear eyed prioritization of risk, based upon a clear strategy for minimizing risk, and based upon a commitment, that we apply all of these strategies to the broader challenge of protecting and securing our infrastructure against a wider variety of threats, the threats that come simply with the passage of time or with Mother Nature.

The recent Gulf Coast evacuation we had last week was a successful evacuation, because we spent three years planning for it, building for it, and continuing to work on it even when the lights were turned off and the cameras went some place else. And the result of that preparation wasn't a perfect evacuation, but it was something that demonstrated real progress and made life safer for the people of the Gulf Coast region.

If we use this approach, this long term focus on the general issue of infrastructure, we will not only have done a service to the people in office when that next catastrophe comes, and believe me, it will come in one form or another, but we will have done a service to our children and

our grandchildren, which is, after all, I hope, the reason most of us in public service have decided that we want to commit to doing this kind of work. Thank you very much.

MR. O'HANLON: Thank you very much, Mr. Secretary. We have about ten minutes for questions. I'm going to take the prerogative to ask the first. I, however, want to thank you as we near September 11 for what you and your colleagues have done to protect the country, although I also want to salute and thank you for your attitude, if not resting on any laurels, or suggesting that there are any to rest upon, but emphasizing all the work still ahead. I want to have one question, this is of your speeches, I think the only one you're giving inside the beltway, so let me ask an inside the beltway question about the state of the Department of Homeland Security, which, of course, was created only five years ago, and it's a big organization brought together, 22 agencies, how is it doing in terms – in your eyes in terms of its ability to tackle the kinds of problems you discuss today; what's the state of the institution?

SECRETARY CHERTOFF: You know, from an organizational standpoint, the most challenging thing for us and the most important thing for us was to build the capability to bring the seven major operational components together for purposes of joint planning and joint operational execution.

And, you know, one of the acid tests of this, frankly, was last week. We were able to bring into one place, through our Operational Coordination and Planning Office, all of the major operational components. Obviously, FEMA had the largest role to play, but including the Coast Guard, Customs, and Border Protection, we had a joint set of plans, we were able to execute plans jointly in a coordinated fashion. You know, if you went back over the last couple of days, you saw not only FEMA being involved in evacuation and in making sure that we worked with the Red Cross and the state and local government in terms of sheltering, but we had the ability to get Coast Guard in there to literally follow the path of the storm in.

I actually got a – I had a direct conversation with one of our Coast Guard helicopter pilots who told me about flooding that he saw as the storm was still impacting, and they were flying in 40 mile an hour winds. At the same time, we were able to take a Customs and Border Protection unmanned aerial vehicle and use it to survey the power lines, so we could help tell the power company and the state and local government, you know, where there might be problems with the transmission lines.

So I would say that, you know, integration is an ongoing process, but if the test of success is what happens in the real world, I think that we have made a good deal of progress.

MR. O'HANLON: Yes, sir, about two-thirds of the way back, and please do identify yourselves, if you could, as you ask questions.

MR. MILLIKAN: Al Millikan, American Independent Writers. Has the opportunity arose yet for local residents and environmental groups to engage in serious discussions where their immediate and perhaps legitimate concerns need to be confronted with the Homeland Security and infrastructure safeguards such as what you mentioned had not taken place in New Orleans before Hurricane Katrina?

SECRETARY CHERTOFF: Well, you know, we deal with all kinds of stakeholders, we deal with community groups. Depending on what the nature of the infrastructure is, we do deal with environmental groups. Actually, what happened in the issue of the barriers prior to Katrina, it wasn't a lack of engagement, it was that the process simply stopped because there was opposition by some of the lake owners and some of the environmental groups.

And, you know, it's a very hard balance between engagement and talking, but then ultimately making a decision on the one

hand and engagement and talking that leads to more engagement and talking and more engagement and talking.

I guess what I'm trying to say is, there is a very serious transaction cost if there's endless discussion. One of the challenges we have to face in this country is that our ability to complete major projects has become very, very difficult because there is so much process involved in getting a decision that years go by. There was a recent piece in the paper about Ground Zero; well, it's been seven years and we don't have – rebuilding Ground Zero in New York, and that's been because everybody has their own point of view. That's great to be heard, but at some point, if the discussion is endless and never comes to resolution, you never get a Ground Zero building, and that's much more dangerous when the failure to reach a resolution results in not building a barrier that, at the end of the day, probably did more harm to the lake front people and the ecology than would have occurred had a barrier come into place.

Bottom line is, we have got to be prepared to have a reasonable amount of discussion, but also to make decisions.

MR. O'HANLON: Yes, sir.

MR. SMITH: Hi, my name is J.J. Smith from H.R. News. The industries that I've talked to are terrified of I9 audits; how can they be

convinced that audits concerning security are going to – they won't be fined for honest errors?

SECRETARY CHERTOFF: Well, you're talking about for immigration violations. We don't fine people for honest errors. People get fined when they knowingly violate the law. Now, there are some people we do do in the immigration area, we do have circumstances where we have raided a business, and it may very well be the business did use all the reasonable tools available to check employees, and the employees were simply using phony identification, you know, that they had stolen from real people. In that case we don't fine the business, but we certainly don't release the illegal workers, we do arrest them and we do deport them, and I understand that has a consequence, but we're not going to turn a blind eye to law breaking.

There's a really easy way to avoid this problem. The way to avoid the problem is, participate in E verify, which is an electronic system, and if you operate in good faith and you use that system, even if it turns out someone has managed to game the system by stealing a real identity, you're not going to get fined or punished.

MR. O'HANLON: Yes, sir, here in the front.

MR. CHERABUL: Tim Cherabul with Telenosis Networks. A lot of the technology that's being developed on the security front is

generating capabilities and information that could also be used within the businesses to improve efficiencies and operations. Is there any initiatives to encourage the development of those technologies so that the same information being gathered to secure the facility can also be used for business operations and improve their bottom line on a day-to-day basis?

SECRETARY CHERTOFF: Of course; our purpose in developing the technology is to meet our needs. Now, we understand the serendipity about this, and I think one of the reasons that businesses are interested in getting into this is because they see the value.

I'll give you a great example, it's in the area of supply chain with maritime cargo. You know, we have an interest in visibility into what is coming into the country in containers, monitoring those containers, scanning those containers, and securing them.

We recognize the industry also has its own reasons, simply because they don't want to have theft and things of that sort. We recognize that having visibility into what comes in through our ports also helps the health and safety of our citizens because it keeps counterfeit goods and adulterated goods out. So there's no question that we can leverage some of these capabilities for broader goals. But I have to say, our typical touchstone is to look at the value from the standpoint of our mission, and if others benefit, you know, that's terrific.

MR. O'HANLON: Yes, ma'am, over here.

MS. CHIATANI: Good morning, Deborah Chiatani GNOT Foundation. Mr. Chertoff, in the light of the fact that all the natural disasters could possibly be man made and directed from narcotics activity in Europe internationally as part of a defacto narcotics, weapons, and crime monopoly, has the Department of Homeland Security secured, or at least coordinated with agencies to provide funding for manpower, and have that type of infrastructure been first, or where is that type of infrastructure supported within the Department of Homeland Security, and what is – excuse me, my question is about the priority, excuse me?

SECRETARY CHERTOFF: If I understood you correctly, you are suggesting that natural disasters are caused by narcotics activity?

MS. CHIATANI: I am suggesting, excuse me, I am suggesting, according to what people have experienced, what people are complaining about in all 50 states, the presence of narcotics bordellos following a pattern, almost programmed in all 50 states, and the known origin of this activity being popular and of popular high end commercialized activity with the signals coordinated and directing and almost predicting weather changes and disasters, key named disasters like Katrina, significant in Russia.

SECRETARY CHERTOFF: -- to say is, narcotics is really bad, and we spend a lot of time interdicting it, but I don't think it has much to do with natural disasters like hurricanes.

MR. O'HANLON: It's a good opportunity for me to say we will try to place all of the Secretary's speeches on our web site, and he deals with other issues such as the MS 13 gangs and narcotics trafficking in some of these previous speeches, as well, so that's an opportunity to mention that. Yes, sir, here in the aisle.

MR. MELACHON: Regi Melachon Nuclear Sect – Nuclear – I would like to compliment you and Assistant Secretary Bob Stefan in putting together an excellent overarching framework through the infrastructure protection plans and the specific plans. I think it's a very good long range structure to work with them. I have two philosophical questions.

MR. O'HANLON: Just one, please, because we only have a couple minutes.

MR. MELACHON: All right. On the spectrum of threats, as you go up the threat spectrum, at some point the threat could be so large that it is way beyond any private sector's capability to neutralize, and if – in the partnership model, if largely the focus is on the private sector neutralizing a threat, at some point on that spectrum it does become an

enemy of the state issue, and the government does have a role, and I'm not clear whether that's really –

SECRETARY CHERTOFF: I agree that – just so you all got the question, the question is, at some point, has the – I'd phrase it a little bit differently, as the consequences of an attack or a disaster become above a certain point, does the partnership model change, because really only the government has the capability to reduce the vulnerability.

I think the answer to that is not so much that the partnership model changes, it's just that the relative role of the private sector in the government changes. For example, when you're dealing with high consequence events, the government is obviously going to play a much larger hands on role across the entire spectrum, prevention, protection, and response. Partnership doesn't mean, again, one size fits all, it means that we work with the private sector to figure out what is reasonable to expect them to protect, and where do we as the federal government and the state government and local government have to get involved in protecting. And we then try to allocate that responsibility in a way that's most sensible and efficient.

MR. O'HANLON: We have time for one last question, and we'll go back here near the last row.

MR. CROWLEY: Mr. Secretary, P.J. Crowley from the Center for American Progress. Kind of a philosophical question; what is your working definition of Homeland Security? You've described today that a lot of your time is spent dealing with things like Hurricane Gustav and so forth, and yet the Bush Administration describes Homeland Security strictly in terms of responding to terrorism. So should the next administration as a review strategy and so forth, you know, look at expanding the definition of Homeland Security so it encompasses all the threats you've talked about today and the all hazards approach you talked about with your department?

SECRETARY CHERTOFF: I guess I would disagree with your characterization of what the administration says. I'm part of the administration, and I think from the very first speech I gave three and a half years ago, I said we were an all hazards agency. And I believe Homeland Security is broadly defined to involve all hazards. It doesn't mean we're experts at every hazard, but it does mean that we have to look across all hazards in terms of coordinating government approach and making sure that we are building a strategy that covers them all.

And the reason for that is this, a lot of problems, a lot of catastrophes don't come labeled, and in many cases, you're not sure

whether something is man made or natural, but the response in many cases is the same.

The protective capability that we're using with respect to terrorism has a lot of spill over effect on protecting against natural disasters. You know, much of the lessons learned since 9/11, much of it has to do with eliminating stovepipes, not looking at things as, you know, particular categories, and failing to recognize the overarching relationship. So here's my definition of Homeland Security, which has been pretty consistent throughout the three and a half years I've been in the job, and no one has ever called me out for using it, so I think it probably represents the administration's definition. Homeland Security is protecting the people of this country in this country against national hazards, whether they are man made or nature made across the entire spectrum of prevention, protection, and response.

Our job is to keep the people of the country safe and secure, whether the threat is natural or man made. We've got to try to prevent it if we can. If we can't prevent it, we've got to try to reduce our vulnerability and harden the target so that the damage is minimized, and then we've got to be able to respond in order to mitigate.

Whether it's terrorism or whether it's hurricanes or whether it's pandemic flu, the strategy is going to be implemented in a different

way. But the overarching approach that all of these are things we have to be concerned about is, I think, a comprehensive view of Homeland Security, which is certainly my philosophy, and certainly I think the philosophy we've tried to embed in the department over the three and a half years I've been here.

MR. O'HANLON: Please join me in thanking Secretary Chertoff.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

/s/Carleton J. Anderson, III

Notary Public # 351998
in and for the
Commonwealth of Virginia
My Commission Expires:
November 30, 2008