

INTERNATIONAL COOPERATION IN HOMELAND SECURITY

May 19, 2005

The Center for Strategic and International Studies

Participants:

David Heyman

Director, Homeland Security Program
CSIS

John Hamre

President and CEO
CSIS

Michael Chertoff

U.S. Secretary of Homeland Security

David Heyman: Good morning. Thank you all for coming here at the early hour of 9 o'clock. Mr. Secretary, or I guess it's "Judge Secretary", members of the diplomatic corps, and distinguished guests, thanks for joining us, and welcome to CSIS. I'm David Heyman, I run the Homeland Security Program here and I just want to say a little context of what we're doing today.

This morning we welcome Secretary Chertoff before he departs for Europe later this week. I think it's appropriate in advance of that trip that we have a little discussion on the international dimensions of homeland security. If there's anything we learned from September 11 attacks it's that terrorism is a trans-national endeavor, and that the 9/11 attackers as we know conceived their plans

in the Philippines, planned them in Malaysia and Germany, recruited from Yemen and Saudi Arabia, trained in Pakistan and Afghanistan, and carried them out in the United States.

And if terrorism doesn't stop at our borders, homeland security must reach past our shores as well. With globalization and the melting of borders and the merging of domestic and foreign interests, it means that we must forge new partnerships here at home and abroad. If over the past couple of years, homeland security effort here has been primarily inward-focused it's not a surprise, but it now must fully embrace the international dimensions of security.

And similarly I would add that the military has been primarily outward-focused and it must now provide greater support at home.

To discuss these issues, and the broader international dimensions of homeland security, we're very pleased to have the Secretary here today, who I would note is sporting the traditional homeland security beard, and to welcome him here today, the President and CEO of CSIS, John Hamre, and we'll be doing questions after this.

John Hamre: Thank you, David. And thank you all for coming. I'm glad so many of you are here. As you know, the Secretary's boss threw a curveball yesterday and moved up the Cabinet meeting and so we had to move this session up. And I at the time thought, "oh God, we'll never get anybody there", you know? And I think it's a real testament to everybody's curiosity about you, that they wanted to come to this session. (laughter)

And in all honesty, you're going to be, all of you, colleagues in the audience, are going to be just wonderfully surprised. This is a very fine leader for this department, and the kind of leader we need right now. You know Washington is filled with people who say they were offered a job but decided to turn it down, that's Washington. We're very lucky that the kind of person that we need right now said yes, and that's Secretary Chertoff. He has the kind of background that's crucial at this time. He does not carry the baggage of biases that so many in the security community bring to this job, and he brings a very deep consciousness about the expectations that we provide a safe America, and an America that is comfortable with our civil values and civic values. This is a man who has dedicated his life to that. We're very lucky. We're very lucky that he's been willing to take this assignment. It's not a thankful job, it's a thankless job, but we're thankful that he's taken it.

I introduce to you now Secretary Chertoff, Secretary of Homeland Security.

Michael Chertoff: Well, thank you everybody, for turning out at this early hour. John, thank you for that warm introduction, and David thank you for your remarks which actually anticipated virtually my entire remarks, so I'm done. (laughter) Actually I have not prepared a speech, what I think I will do is outline some of what I envision as being the international dimension of what we do, as I look forward to my first trip overseas, I guess yeah, it's my first trip overseas in this job, coming up next week.

And I think it is significant to me at least, to be here, because I know what

fine work this CSIS has been doing, for years it's been an important forum for debating, and having dialogue about strategic issues of global importance. I remember seeing Secretary Ridge, I think I watched it on C-Span, shortly before he went on his last trip to Europe, talking about what he was going to bring with him on the trip, what he had learned over his two years in the department, and so it's, seems appropriate for me to be here to talk about what my vision is as we go forward, in terms of dealing with the homeland security question outside the homeland, abroad.

And before I begin I really do want to pay a brief tribute to Governor Ridge, who did a phenomenal job with Admiral Loy and everybody else who were the original, I guess what they call plank owners, of the Department of Homeland Security, because they really built it from scratch. And although we are currently engaging in a review, looking to making some adjustments in terms of maybe organization and mission, the fact that we can be in a position to take this kind of a review two years into it, is a testament to the very fine foundational work that was done that leads us up to this point. And I would be remiss in not dealing with that.

I think as David pointed out, we know that terrorism is preeminently a global threat. There are obviously domestic characteristics to terrorism, but in terms of what the public is concerned about, and certainly what the department was formed in order to address first and foremost, it is global radical terrorism.

And as Thomas Friedman said recently in I guess his latest book *The World Is Flat*, it is really, terrorism in the twenty-first century is really the globalization of the kind of terror acts that we saw in the twentieth century. And much as globalization has transformed the world of business, it has transformed the world of terror. And so we need to think about how we confront terrorism by looking at twenty-first century structures and characteristics that terrorists exploit in order to carry out their missions.

As David pointed out, 9/11 itself is a great example of this. We're talking about a plot that was hatched in Central Asia, with recruits who came from Saudi Arabia, who were trained in Afghanistan, who set up and began to develop their infrastructure and their platform in Europe, and then who carried out and executed their mission here in the United States. That is globalization. That is networking. That is outsourcing. That is all the characteristics of twenty-first century organization that we're accustomed to thinking about in the context of international business, but that unfortunately is also available to those who want to commit acts of international terror.

So we are fighting a different kind of a war. It's not a war that we are going to win in the same way that we won World War II, by massing superior forces in the field, or even the kind of war that at least the first part of the campaign in Iraq was, where we bring in superior air power, mobile forces, and then we crush the enemy. This is fighting a network, and so as we talk about a strategy to deal with global terror, we have to think about what is a strategy for dealing with a network. And clearly one way to look at it is we have to create our own network, to compete with that network, and to combat that network.

We also have to look at what vulnerabilities networking has, and those

vulnerabilities tend to be things like communication, transportation, movement of people, movement of cargo. Those are the kinds of activities that bind a network together. If you think about, for example a benign network, a global business, you have to communicate with the various parts of the business, you have to move people and goods and services, and that's how a network works in a positive way. In a negative way as well, of course the terrorists exploit that strategy to carry out their missions, and so we need to look at the peculiar vulnerabilities that networks have, and that is this connective tissue that allows bad people and bad stuff to move back and forth internationally.

What that tells us right away is, that if we're going to challenge the kind of interdependence that a terrorist network thrives upon, we have to be able to confront the network everywhere it operates, and that means we have to be able to function internationally, and do it in part (inaudible) with our overseas allies. And I don't think this is a new insight, we've certainly had movement in this direction over the past couple of years.

The Department of Homeland Security, and before that the various elements that make up the department, were talking about, with our overseas allies, about issues like container security, passport security, and increasing our ability to have biometric and secure travel documents, exchange of information about travelers, so that we could anticipate who might be coming in and block those people that we don't want to have coming in.

In my own prior job, as head of the criminal division of the Department of Justice, we put people overseas, to work with prosecutors and investigators in Europe, precisely because we needed to build up a network of law enforcement that would parallel the network of terror. So this is not new, but as we are poised here two years after the department was formed, it's a good time to think about, how do we take this to the next level, how do we move beyond simply partnering on an individual episodic basis to building a true partnership that will operate in a mission-oriented focus, where we will work together with our allies overseas to accomplish a mission that will secure the entire world.

And let me tell you where I would like to see us go with this, at the end of this next stage of development. We need to have a world that is banded with security envelopes. Meaning, secure environments through which people and cargo can move rapidly, efficiently, and safely without sacrificing security. And in that kind of a world, it would be possible, with the proper security vetting, with the proper technology, with the proper travel documents, with the proper tracking of cargo, to move relatively freely from point to point all across the globe, with the understanding that those within the security envelope, we have a high confidence and trust about, so that they don't have to be stopped at every point mechanically and revetted and rechecked, and those outside the envelope would be those on which we could focus our resources in terms of the kind of in-depth analysis and the kind of in-depth vetting that is necessary to make sure bad people can't come in to do bad things.

So that is ultimately the vision of where we go, and I think it's one which would happily not require a sacrifice of liberty or privacy in order to promote security, it's one that would maximize all of these values, which is of course again

what our ultimate goal is, is to preserve our lives but also to foster our way of life.

And let me talk specifically about three areas in which I think we can start to concretely move forward, as we try to develop this worldwide security envelope. First of all, the issue of screening. We have to have a systematic approach to screening that meshes with the approach taken by our overseas allies, that takes advantage of modern technology, and that gives us a real sense of confidence that we are screening out bad people.

Right now we are using the most primitive kind of screening in many respects, meaning we screen for bad names, and of course names are not the best way of identifying people, they're certainly not as good as biometrics. We screen with technology and by hand searching for certain kinds of bad cargo. We are starting to move forward using somewhat more technologically advanced devices at our ports, that now allows that we would look inside cargo containers without actually breaking (balk?). We're starting to use more sophisticated methods of screening that rely upon getting information about cargo, and using that to sort out what the most high-risk cargo is, and then focus on that high-risk cargo. So we are starting to develop more sophisticated tools, but we really have to press that forward. And that's going to boil down in the first instance to the question of information sharing.

We are going to need to have better information about trusted travellers, if we are truly going to move to the security envelope, where people can move freely, but with the sense that we can trust them. Now that means that we need to get information not only from within this country but from abroad about people who are travelling. And that runs into some important cultural and legal challenges. For example, although we all, I think we here in the United States and our allies overseas believe in the importance of privacy and liberty, we sometimes define how these values get implemented in somewhat different ways.

The issue of data protection, for example, as we deal with it, is sometimes a little bit mismatched with the way the Europeans do. So we need to start to think of ways to get congruence between these sets of values and to translate them in a way that allows us to operate together. It's my contention really at the end of the day, if we had a true system for providing necessary passenger information in advance of travel, securing it against improper or inappropriate dissemination or distribution, that that would actually foster privacy. That we would have less intrusive checking at the border, checking at the doorway to the airline, easier travel which means a greater sense of freedom, so that in the end we would in fact be fostering all the things we want to foster. But we need to get by some legal and cultural mismatches in order to get to that better position. So that's step one.

I hope that we can go to Europe and go overseas and start to talk about how we can finish the process of getting our information shared appropriately, and with due respect for peoples' privacy. Second, technology is obviously going to be critical. We need technology for screening cargo, we can use it for screening people as well. We're doing a lot of work in this country, Europeans are doing a lot of work, we ought to make sure we get on the same page with

that work for two reasons. First of all we maximize our resources if we have fully available to us all of the ingenuity and talent across the globe of people who are thinking about ways to use technology.

Secondly, we've got to be compatible. It doesn't make a lot of sense, for example, to have radio frequency chips that use different kinds of modalities in the United States than in Europe and in Asia, because we're simply going to make it hard for us to interconnect. So that to the extent that we can start to build common platforms and common technological approaches, again we will move ourselves closer to this concept of a security envelope. And we will also save ourselves some money, and some effort, and some time.

Finally law enforcement. As I've indicated, intelligence sharing and law enforcement sharing has been critical to dealing with the threat of terrorism globally, we need to continue to advance on that front. We've done a lot, I know for example in Europe, the Europeans themselves through the EU mechanism, Eurojust and Europol, have been working to try to have greater connectivity among their various law enforcement agencies and intelligence agencies. We need to build on that, we need to encourage it, again because that free flow of information and cooperation gives us an ability to network in a way that lets us match the network of the enemy.

So these are the three principal areas that I hope to start to dialogue and talk to our European partners about when I go overseas, I think this is the first step in what has to be ultimately a worldwide effort that gets us to this notion of a security envelope. And I think it's important to us as Americans because in the end, we have to make sure that what we are doing to defend our homeland is consistent with our vision of the way the homeland has to be. We don't win the war against terror if we destroy those things which we value in our own lives. We win the war on terror by being able to conduct lives, encourage prosperity, protect liberty, preserve privacy, while preventing terrorists from carrying out actions in this country.

So we don't want a fortress state, but we want to have a state that is open, that encourages the historic flow of students coming into this country in order to get an education, I mean that is a huge and important part of the war against terror, is bringing people into the country and showing what we have to offer. And so we want to have more of that, we just want to make sure we do it securely. Trade -- we are a great engine for trade, we are creative, we have an enormous amount of energy, we want to make sure we are not slowing up or blocking the channels of trade because we are not smart enough in terms of how we protect ourselves against bad cargo.

All of this, then, is the vision that we have to keep in front of us as we work specifically on creating this worldwide security envelope. At the end of the day of course, it boils down to something that I've spoken about previously, and which I know many of you here have talked about, which is risk management. We have to go into the process of balancing all of these characteristics, recognizing that we are always going to be managing risk. There is a perfect way to avoid risk. If you want to avoid risk to ports, you shut ports down. If you want to avoid risk to air traffic, you never have air traffic. But we all realize that's foolish and self-

defeating.

So in order to strike the balance we want to strike, and create an appropriate security envelope and not one that is clogged and dysfunctional, we have to again always use risk management as a philosophy.

So with that being said, I am very much looking forward to my upcoming trip, I'm sure I'll have interesting observations and opportunities to meet with my colleagues overseas, we've got people in countries all over the world that have contended with terror for many, many years and have tremendous insight, not only into the technology and the process, but also the psychology of how a society deals with terror, and so I'm going over to learn and to listen more than to speak and instruct, but I'm hoping we can begin this dialogue of moving our partnership to the next level and creating this worldwide security envelope.

I want to thank David and John again for inviting me here, giving me an opportunity to kind of preview what I'm hoping to achieve, and I guess we have some time for questions. (applause)

David Heyman: The Secretary will now take questions. Please identify yourself, there's microphones in the room and they'll come forward. Sir.

Question: Thank you Mr. Secretary for this opportunity. I guess while talking about law enforcement with the rest of the world, one question now, how about the issue of rendition of prisoners. Could you tell us if so far it was effective as a policy, have there been any good results?

Michael Chertoff: Well, of course there are various legal authorities and requirements that govern the way we treat prisoners. Let me step back and put the issue in context. The principal weapon we have in the war against terror is information. In World War II we had radar. Radar told us when bombers or enemy aircraft or enemy ships were coming in, we could combat that. There is no radar against terror. Even these screening devices, no matter how technologically advanced, are only an imperfect way of warning us so that we can intercept and prevent. So we do need to have strategies for getting information, and dealing with intelligence so we can anticipate in advance how to save lives.

We do that in a way that is consistent with the law, but we need to be mindful of the fact that getting information, getting intelligence, is the number one way in which we anticipate attacks and save human lives. If we didn't have intelligence, I'm afraid that the death tolls would be much higher, and the impact on societies across the board would be much harsher. Yes.

Question: I'd like to know... I'm doing my doctoral dissertation at AU, and I'm working on terrorist financing issues. What is the degree of cooperation you're getting post-title III of USA Patriot Act with the other departments, the DOJ, the Treasury, and State, and so on. And how do you affect [inaudible] group of banking standards. What's the degree of collaboration [inaudible], and how are things going right now?

Michael Chertoff: Well we do have a lot of cooperation within the United States government of course, there's traditionally there's always been issues involved in making sure we're working together. I think we're much further along

with that than we were two or three years ago, inside the U.S. government. You're right to point out that this is an international effort, we've been working with our counterparts overseas. In many ways we have a very good working relationship, sometimes we have differences of opinion about where the particular groups should be treated as terrorist groups in terms of financing, and whether they ought to be on lists that require monitoring, or even in fact require shutting down channels of money, so we have to work through some of those issues. But -- and of course we have the so-called off-line methods of transmitting money, including hawala and things of that sort, which we have adapted ourselves to deal with.

But I do think there's been a tremendous amount of progress and I've read recently, and I've forgotten which institute reported on this, that in fact there's been significant progress made. But you know, money is like water, it finds a way to get past barriers if there's any crevice or crack, and again, this is an area where networking and technology will help us a great deal in terms of choking off the flow of resources that allow terrorists to carry out their operations.

Question: Andre [inaudible] Tass News Agency of Russia. Mr. Secretary, are you planning to visit Russia while in Europe, and if so, whom are you going to meet with, and what issues would be on the agenda, and how would you describe the level of cooperation between the two countries on security issues in general, and on information sharing in particular? Thank you.

Michael Chertoff: That's a lot of questions. Russia is not on the agenda for this trip, which will be a short trip, although I'm hopeful that at some point in the future I will be able to go over there. I did actually take a trip to Russia when I was head of the criminal division, with the Attorney General, and we had a very good set of meetings with our counterparts over there. I think it underscores again the fact that we all deal with terror and terrorists. Sometimes the particular variation that a particular country deals with is different, but you know the terrorists are networking now too. And there's a bit of a tendency I see sometimes in the press or in the media to focus on for example, Al Qaeda, as if it is a stand-alone, formal organization like a corporation.

Again I want to drive back to this idea of a network. While there is an Al Qaeda, it is also a network with other organizations, including organizations that obviously have impact on Russia, and of course we are very mindful of what happened in Beslan. So we are always working again to improve our information flow, I think that everybody now has an understanding that this is a global threat. Sometimes there are obviously hiccups in the process of keeping ourselves informed, but the intent, and the desire, and the recognition of the importance, I think, remains. Yes.

Question: Armand Peschard from CSIS: I was wondering if you could comment on the work of the, I think eleven, working groups that you chair under the security and prosperity partnership of North America, and to what extent is inter-operability being emphasized in the work of the working groups?

Michael Chertoff: Well of course, just to remind everybody, the SPP, the Security and Prosperity Partnership was announced by the President, with the President of Mexico and the Prime Minister of Canada, in March in Crawford, we

were there. I think it is... all three heads of state view it as a very important initiative because we have a unique relationship since we are part of the North American continent. We have a common perimeter, we have obviously very robust trade relationships, and we therefore have certain unique common security and prosperity issues. We're working very hard on those issues, and I think we're due to report towards the end of June on our progress. I can tell you I spent a fair bit of time on it, I know I've spoken to both my counterparts both in Canada and in Mexico on a regular basis about it, and I think it's an important opportunity for us, first of all to make sure that the huge volume of trade between our countries does not diminish because of the need to make sure of security, but at the same time making sure that we are working together and cooperatively in terms of information exchange, in terms of common protocols at the perimeter about how we handle cargo and passengers, so that we don't have seams or cracks between us that can be exploited by terrorists.

You know, sometimes people say, treat security and prosperity as if they're trade-offs, where one is a win, you know it's a zero sum game. I think quite the contrary. Without adequate security we're not going to have prosperity. I think we know that if there are incidents that result in serious terrorist consequences that are attributable to some individual or some commerce that came across the border, that is going to have a negative reaction on commerce, it's going to have a tendency to close the border up to some degree. We don't want that to happen. So prosperity depends on security, but at the other extreme, security without prosperity is pointless. So this is kind of a concrete area where we're working, to make sure we move both of these values in tandem.

Question: Thank you, Mr. Secretary. Nat Thomas with CIRRA [ph] Given the emphasis that you've placed on technology in the fight against terrorism, what plans does your department have for more fully utilizing the research and development being done at our universities here in the U.S. and abroad to fight against terrorism, beyond the centers of excellence that are already being established. Thank you.

Michael Chertoff: We have obviously a science and technology directorate, which was written into law precisely in order to leverage our ability to encourage science and technology, which is the key to, I think, it's really our competitive advantage in dealing with terrorists. And there's also something which we call SHARPA which is the homeland security advanced research network, which again I think we need to make sure we are adequately exploiting in order to encourage the development of the correct technologies. You know we have various kinds of programs with universities, we have the tremendous capabilities of the national laboratories, which not only deal with technology in a narrow sense but deal with systems, and proper thinking of how do you create systems that would ensure better screening and better protection for the country.

I've met with, in the course of my three months on the job I've made it a point to meet with scientists and technology people, private and public, to get a sense of what is out there. And there's tremendous opportunity for us to harness the energy and the creativity of the private sector, and academia to build not only just individual items of technology, but systems of technology that will give us leverage and will give us the upper hand in this kind of asymmetric warfare that

we deal with with terrorism. Yes.

Question: Hi, David Silverberg, HS Today magazine. You mentioned earlier the review that's ongoing now. What's the status of that review, is there an end date in sight now, and will you be announcing all the results at one time?

Michael Chertoff: The first question takes a little longer to answer. The answer to the second is yes, and the answer to the third is no. The status of the review is this. I had directed that the groups working on this, report in to me, be prepared to report into me, by the end of this month, and we are essentially on track to get that done. What I anticipate will be happening is I will be sitting down with the various groups that are working on elements of this review over the next weeks, and discussing and working out what the suggestions are, how we ought to react, and starting to develop proposals for moving forward on those things. This is not going to result in unveiling a printed report that then gets put out. It's rather going to be a template and the strategy for going forward over the next months, across the board, dealing with all the missions of the department and all the department's responsibilities.

I have no doubt that there will be some aspects of this that we will unveil probably very early in June, some may take a little bit longer. The purpose of this was not to produce a single document that could then be published and sent around, but it was really for me and the leadership team at the department to be able to look across the board at what we're doing, figuring out what the gaps are, where we need to make some changes, and also really working out some substantive policies. It was a great opportunity I think for people in a cross-cutting way, from different disciplines, to think outside the usual categories, not to be constrained by what they think is possible or acceptable or conventional, but to really talk about what would you do if you could take a fresh piece of paper, knowing what we know after two years, how would you draw a mission plan, an operations plan, to get where we need to get.

I think, my impression is there's a lot of energy and excitement in the department about doing this. I've actually started to sit down, and get a preview of some of what the findings and the suggestions are, and I think we will produce from very interesting and important results in terms of mapping our next months of activity.

Question: Bill Courtney, CSE. In the defense context, the kinds of goals that you outlined for your European trip, we pursued in NATO for a half century, both the technological cooperation as well as the political impulse to assure the technological cooperation takes place. Do you foresee for homeland security and counter-terrorism a need to have, if you will, a large international, super-national organization, that can have both a political and a technical dimension to achieve its goals?

Michael Chertoff: No. I think this is really about networking. There are a lot of multi-lateral institutions. You know, the EU obviously is a point of contact for us, as are the individual bilateral contacts. We have had a long-standing superb relationship with the British, our allies in Britain, Australia, New Zealand, Canada, we have a very good relationship with Mexico. I don't know we need to build more bureaucracy, I think what we need to do is network with the existing

structures, and have a clear vision of what we want to accomplish, and then move on it.

Question: Andrew Howell, with the U.S. Chamber of Commerce. I want to follow up on one of your three areas, that of screening and registered travellers, specifically as you may know there's going to be a pilot program in Orlando, with a private sector company running a registered traveller program. How do you envision in this process the role of the private sector going forward, is Orlando the beginning of a larger set of private sector initiatives to screen travelers and provide tangible benefits to them, or do you view that as kind of the traditional, now I guess what TSA has done so far in registered travel, a more traditional government role?

Michael Chertoff: I don't think we necessarily are limited to a traditional government role. I mean, there are a number of ways in which the private sector can really add value and play a major role in this process. One is of course technological, I mean to the extent we have tools that are more efficient in screening, that's often an area where the private sector contributes. Second, where we do -- and I want to be very careful about how I say this -- where we do screening, and we do need a certain amount of limited information for screening, some of that's available in the private sector. Now it may be that it should remain in the private sector, that we don't want the government to accumulate a lot of data, but that we want to figure out a way to deal with the private sector so that we can get a signal or a flag that there is, for example with respect to a traveller, a reason to be concerned, without actually having to dive into the underlying data and get access to things that I think people might be reluctant to have the government see. So I actually think the private sector can help us construct an architecture that will be privacy, pro-privacy, and privacy-protective, while giving us the ability to see results that would be important in terms of deciding who we have to focus on.

Finally the private sector can deal with it this way: You've got a lot of people travelling, almost always for private business. As we talk about trusted traveller programs, getting more of the kind of information that allows us, for example, to let people move freely through airports, as we talk about biometric types of identification, which maybe become available on a kind of voluntary basis, the private sector can create a marketplace for this. If people in fact see value in having a biometric card, and volunteering some information for it in return for getting some kind of trusted traveller status, that will create a marketplace for the technology, and a marketplace for the systems that we need to drive that forward, so that's another area where we look to the private sector.

Question: I wanted to ask another question about collaboration with the private sector in screening, but a different kind of screening, and that is screening for job applicants, for particularly sensitive positions, for example in critical infrastructure. And what your thoughts might be on the practicality, value and feasibility of screening those applicants against information that the government may have with respect to whether it's the NCIC or eventually, if they become reliable enough, some sort of terrorist watch list.

Michael Chert off: Well, we have, again, we have pieces of this on the

drawing board. I mean there is a TWIK program, a transportation workers card which is designed to deal with people who are going to be transporting hazardous materials. We have of course, government buildings have various kinds of screening devices. At the end of the day, again I think you do want to have a capability to screen people who have access to critical material, either when it moves or when it's housed someplace, nuclear power plants for example, and I think you want to build a capability that has the following aspects: First of all, that does check against databases that are accurate, and that means not just name databases, but biometric databases, so that we can determine if a person in fact is secure. And by the way, you want an ability to update that, so that if you get something, information about a person in year one, and the person, something happens and they become a terrorist in year eight, you're going to find out about that. And I think you can build that, because your platform ultimately is a verifiable card, which has a biometric so that we know, a person, once cleared, and once vetted, we know the person who is coming in is in fact the person who they say they are, you can do that with fingerprints, for example. You can build into the card an RF chip, or some kind of a capability so that if in fact the status changes, you can somehow decommission the card, or you can put a red flag on it.

These are technology solutions, but they're really broader, they're system solutions, and in the end if we create this kind of a platform, in theory it could roll out in the transportation area, in the critical infrastructure area, nuclear power plants, government buildings, and if we have it, although we don't want to merge them necessarily in one data base, if there's some interoperability and a capability of speaking across the platforms, you might be able to carry a single card that would get you into a courthouse, get you into a government building, and get you into your job, and at a minimum of invasion of your privacy and interference with your freedom of movement.

Question: Much seems to be made from some countries, particularly European countries Mr. Secretary, with respect to the different perspective on the international anti-terrorism activities. Some European countries particularly seem to be concerned about what they see as an undue emphasis on the war, about war on terrorism, versus a multi-disciplinary, multi-agency approach. Do you see that as an actual impediment to international cooperation, and how do you see, will you comment on that kind of an issue?

Michael Chertoff: Well, there may be different views about how you think about what we do. I have no doubt that we are in a war, and I don't know any way you could define what happened on 9/11, the fact that bin Laden declared war on us, the fact that he tried to blow up an airliner with a shoe bomber, the fact that we have some bombings in Bali and Madrid, I don't know how you could define that as anything other than a global war.

But I think at the end of the day, even if there are different ways of talking about this, in Europe and other parts of the world, we can get beyond that, because I think we all want to achieve the same result. And by the way, I think this war is a multi-disciplinary war. The first line of defense is the president's strategy to take the war to the enemy because, not only do we get valuable intelligence, but if they're worrying about themselves, they're having less time to

think about how to plot against us. So that clearly, I mean I have no doubt that as a principal element of the strategy of fighting the war, the president is absolutely right in taking us overseas and fighting the war over there. But we use all the tools, and I think, you know, we've always talked about giving the President, and I think this applies to foreign leaders as well, all the tools in the toolbox, and that includes domestic law enforcement, it includes science and technology, it includes all the dimensions of what we can bring to bear including financial resources, and diplomacy. So it's a war fought with a, perhaps a different or a broader set of tools, and I think that we can all internationally agree that we need to get this thing done, even if we want to talk about it in slightly different ways.

Question: When you talk about the desire to create the security envelope - - I'm Eric Clifton from the New York Times -- what kinds of information from the Europeans and what categories and for what purposes would you like to try to be able to have access to, to create this global security envelope? What are some examples, if you could, please.

Michael Chertoff: Well, for example, if you're dealing with cargo, let's take shipping cargo and containers, one would like to know, for example, as much as one can know about the constituents of a particular container. You know, you can go to FedEx, or UPS, or other kinds of freight-forwarding and shipping companies, and they have a phenomenal ability to track information and monitor, they can tell you where your package is, you know your own columnist Thomas Friedman describes this in his book, about how great UPS is at doing all this stuff. Well, can we use those kinds of systems when we're dealing with shipping material through containers into ports, to determine, you know verify who in fact the manufacturer is, what the product is, track that as it moves through the shipping system, until it gets onto the ship, or better yet when it arrives at the final port of embarkation, so we know what needs to be inspected physically and what we're confident about can just be moved through, that is an example of getting the kind of information that is currently, by the way, completely available to shippers in the private sector. And building on that kind of a technique, so that when we confront the millions of containers that move into the United States every day, we can be confident that we're inspecting the ones that need to be inspected, and the ones where we have a security envelope, because we know what's in it and we know that there's been protection given to the containers so no one can put something inside of it, sneak something into it, then that kind of freight, that verified freight, can move very rapidly, and I think at the end of the day that's going to be a competitive advantage to shippers, they're going to want to have a program that gives us the kind of information we need to keep cargo secure so it can move rapidly through the system.

Question: Just wondering if you support the Bush administration plans to expand the Patriot Act to allow the subpoena of business records without judges' approval?

Michael Chertoff: Yes.

Question: Could you expand on that?

Michael Chertoff: Yes I do. (Laughter) No, I mean, not to be facetious about it. Getting information quickly is really important, and you know, I obviously

was around when the Patriot Act was passed, I think it has been a tremendous, positive, value-added element of the war against terror. It's allowed us to get information promptly, and it's allowed us to make sure it gets to the right people, and we connect it up. And I think it's been handled in a responsible way. Now, I know that as the Attorney General has acknowledged, there's always an opening to consider calibrating or making adjustments if experience suggests that ought to be done, but I think that it is an important weapon in making sure again that we have available to us the most important tool against terror, which is advance information and knowledge that we can use to intercept and prevent a terrorist act. Thank you very much.

David Heyman: Thank you, Mr. Secretary. We look forward to continuing to dialogue with you, we wish you good speed on your next journey. Thank you.