

## Proceedings of the April 5th Senior Advisory Group Meeting and Participants List

"These problems all stem from the fact that the United States won the Cold War, and they must be understood in that context. Our pre-eminent military status means that enemies know that they cannot attack us directly. No one will do what Saddam Hussein did and line up tanks in the desert to face the fury of the U.S. Armed Forces. Instead, our enemies will attack us where we are weakest: here, in the homeland. These are the sort of challenges that come with being the world's only remaining superpower."

- Dick Clarke, National Coordinator for Security, Infrastructure Protection and Counterterrorism

**DR. JOSEPH COLLINS, Project Director:** Welcome Governor Whitman, thank you so much for flying down from New Jersey. Senator Robb, we appreciate you reserving the room for us and being a member of our group. Congressman Dicks, thank you for coming and agreeing to speak this morning. We also have a number of other folks from the Executive Branch this morning that will advise our group. Among them is my old friend Neil Gallagher from the FBI. Pam Berkowsky is our Department of Defense point of contact. Pam has contracting authority so I must tell you that her lawyer said that although she will be at all of our meetings, she is not allowed to be an advisor. Finally, Ambassador Michael Sheehan will be our State Department representative. Unfortunately, he could not join us this morning.

There are lots of other folks here who are old CSIS hands. One who has been involved in nearly all of our major efforts over the last five years is Jim Woolsey, former Director of the Central Intelligence Agency (CIA). Thank you for coming, Jim.

Why did CSIS start a major project on Homeland Defense? The answer is simple. The nature of international relations has changed, and so has the nature of many of the tasks associated with national defense. For most of the last fifty years, national defense was mainly about foreign threats that menaced our allies and our forces overseas. Today, with the proliferation of Weapons of Mass Destruction (WMDs), new forms of terrorism, and the vulnerability of our critical information infrastructure, national defense may well involve deterring, fighting, or even just coping with non-state actors who can directly and devastatingly attack the U.S. homeland. In short, we must think about a relatively new class of threats and assess how we should meet them, not just at the federal level-which is where national defense has mainly been developed-but also at the state and local level.

We hope to further our understanding of these new tasks through a three-part initiative. The first stage in our work will be an independent study by Dr. Tony Cordesman, which will cover current conceptions of Homeland Defense. Most of you know Tony from his years working for Senator John McCain or from his many appearances as a military expert for ABC News. Tony is also the Co-Director of the CSIS Middle East Program.

The second stage will consist of four independent study groups: one on missile and air defense, headed by my colleague Dan Gouré; another on terrorism and WMDs, run by Frank Cilluffo; and a third group on cyber threats led by Arnaud de Borchgrave, who runs the CSIS Transnational Threats Initiative and is also the president of United Press International (UPI). I will lead the final study group on policy integration.

Tony Cordesman and the chairs of these study groups will issue their findings by the end of the year. Their work will contribute to the development of a Senior Advisory Group report scheduled to appear in April 2001, just in time to advise the new administration's policy review.

Please do not think that CSIS has all the answers and just needs help getting the word out. We do not have all the answers. Rather, we are soliciting input from you and from your staffs, and we hope that some of your staffers will help us with our research. To that end, contact information for

all of the experts I mentioned earlier is included in the packets we distributed to you prior to this meeting.

That ends my boring walk through the group's charter. The rest of the program this morning will be more exciting. Our next four speakers, John Hamre, Dick Clarke, Representative Norman Dicks, and Representative Curt Weldon, will give us their views on Homeland Defense.

John Hamre will speak first. He has been the president and CEO of CSIS since Monday, April 3rd, and he has already made many substantive changes. [Laughter] Anyone who works his way up from the policy foxhole to be the Deputy Secretary of Defense is likely to have something important to say on this set of issues.

**JOHN HAMRE, President of CSIS:** Good morning. I must confess that this is a very awkward situation for me. I am so new to CSIS that it is difficult to sound authoritative. To speak with my old hat, however, would be dishonest, as I am no longer with the Department of Defense (DOD). Hence, I think what would be best would be for me to speak broadly about the DOD perspective on Homeland Defense.

Homeland Defense is an issue that was thrown in our lap. The President has consistently said that he is not satisfied with our readiness. The concept of Homeland Defense probably means different things to different people. If we were to survey those attending this meeting, we would probably get three, maybe four different factions with different perspectives [on Homeland Defense]. To some it means National Missile Defense (NMD). To others it means protecting the country against terrorist threats using WMDs, be they chemical, biological, or nuclear. Others would stress cyber attacks—a newly emerging dimension of national security. There are still others who will talk in broad terms that include the national counterdrug strategy. All of these issues are linked by a new 21st Century reality. In short, we are now in an era when small numbers of people can now wage war on the United States, and where America's heartland is at risk.

CSIS was asked to see if it was possible to develop a kind of "Unified Field Theory" for Homeland Defense. Unified Field Theory, as some of you may know, is the effort in physics to develop one single explanation for magnetism, gravity, radiation, and other phenomena. I am not sure that you can develop such a theory for Homeland Defense, however, because the issues involved are so different with respect to their possible implications and solutions. For example, nearly 98 percent of DOD's activities in cyberspace are rented capabilities. DOD does not own the U.S. infrastructure that is likely to be attacked. What is more, we do not have the necessary authority to address these issues. Hence, Homeland Defense presents a very interesting set of problems that includes motivating the private sector to worry about security—something they currently see as a cost to business.

Protecting our assets in cyberspace is quite different from the questions posed by the development of an NMD system. NMD is a classic military problem. It requires organizing resources, developing new technologies, working out command and control procedures, and establishing release processes from the National Command Authority. It is a classic military problem.

NMD, in turn, is very different from the threat posed by WMD terrorism. For all practical purposes, preventing or combating terrorism is a question of how you organize the government and its various authorities. The federalism issues that come into play are ultimately the hardest part about WMD issues in the United States. How can the government become effective the moment after we have an absolute catastrophe? How do we maintain an authoritative voice to ensure the public that the world is not coming to an end? How we give people clear instructions about

whether it is or is not safe to leave their homes? What is the relationship between the president and the governors in this area? These are fundamental federalism questions that we must re-explore.

There are two strikingly different dimensions to the WMD problem. The first is prevention—stopping adversaries before they can attack. The second is response, that is, ameliorating the fallout from a WMD strike and reassuring both civilians and American society after such an event. We have an obligation as serious intellectuals thinking about national security to look ahead at this problem that is on our doorstep, but not yet in our home.

You may have heard the analogy of a "cyber Pearl Harbor." The analogy is quite apt, because there was not a single capital ship, by that I mean an aircraft carrier or battleship, that saw service in World War II where we had not laid the keel for the ship before Pearl Harbor. What is more, we maintained those capital ships using a Norfolk, Virginia dry dock that was built in 1938. The U.S. government saw that we would need these tools to protect America, and it took the necessary action. In regards to Homeland Defense, that is exactly where we are as a nation today. We have an opportunity to look ahead while there is still time to develop the basic, flexible capabilities that we will need to respond to emerging threats.

Let me quickly turn to Dick Clarke. No one has been more in the center of trying to get the government to focus on these issues than he has. As you know, Dick is a coordinator for all things dangerous at the National Security Council (NSC). He initially started coordinating the government's counter terrorism efforts and has broadened that mandate to include a broad review of the means of protecting American critical infrastructure.

**DICK CLARKE, National Coordinator for Security, Infrastructure Protection and Counterterrorism:** Thank you for inviting me, John. I think this panel's work will be crucial to the next administration as it sets its priorities in the first few months after the election. Homeland Defense has to be one of those priorities. As John said earlier, this issue comprises several components that must be addressed differently. These problems all stem from the fact that the United States won the Cold War, and they must be understood in that context. Our pre-eminent military status means that enemies know that they cannot attack us directly. No one will do what Saddam Hussein did and line up tanks in the desert to face the fury of the U.S. Armed Forces. Instead, our enemies will attack us where we are weakest: here in the homeland. These are the sort of challenges that come with being the world's only remaining superpower.

In 1993 the United States experienced the first foreign terrorist attack on our territory. The World Trade Center bombing took place two weeks into the life of this administration and forced the President to focus on this issue early on. Two weeks later there was a second foreign terrorist attack at CIA headquarters. It was clear to us then that foreign groups comprised of foreign individuals were coming to the United States with the sole purpose of carrying out terrorist attacks. The situation demanded a response.

The threats associated with cyber terrorism have also focused our attention. Two teenage hackers were responsible for the February 1998 "Solar Sunrise" case. These teenagers were able to get into the Pentagon's unclassified logistics system, download passwords, install sniffers on the lines, and put in trapdoors. They could have crashed the system. Moreover, they were doing this at a time when the President had ordered troops and aircraft to Kuwait because of renewed threats from Iraq. Over the course of that weekend, John Hamre and others initially considered the possibility that Iraq was responsible for these attacks.

That we later discovered that two teenagers were responsible is not good news. It was a great relief at the time, but it is not good news. Subsequent to that event, John ordered a series of security changes that would make that kind of attack difficult but not impossible to prosecute.

That is the low end of the cyber terrorism spectrum. It moves up through extortion, fraud, and industrial espionage. At the far end of the spectrum is war by computer attack. When the NATO alliance bombed Serbia last year, they hit mainly infrastructure. In the United States, the telecommunications, transportation, and electric power infrastructure depend on computer-controlled networks. Each of these networks can be penetrated by a determined adversary.

There is a unique challenge here. For the first time in our history, the armed forces cannot defend us from the foreign threat. They cannot surround the power grid. In discussing these issues Senator Bennett often talks about a steel factory that was built in Utah during World War II. As soon as the factory went up, the Army came in and surrounded it with anti-aircraft guns. Today, he notes, we are asking that steel company to go out and hire a bunch of "[cyber] anti-aircraft guns", and worse yet, to hire the gunners. The U.S. government does not have the gunners. We do not have enough trained information technology security people available to hire. Our educational system has not yet created enough IT security specialists.

Therefore, we are asking the private sector to defend not only itself, but the country as well. And we still cannot tell them precisely how to do this because we have not yet developed the standards and best practices, let alone the software and hardware, necessary to defend these networks.

Despite the clear implications for national security, this is also a law enforcement issue. The FBI now spends a lot of time trying to learn about software and source codes-the sort of things that the FBI did not worry about before. But if every house in this county lacked a front door lock, would the answer be to go out and hire more police? To do so may be part of the solution, but that is not the only possible solution. Unfortunately, that is where we are today. Every computer network in this country lacks a front door lock. We need not only to hire more police and train the FBI to address these threats, we also need to motivate the private sector to buy the necessary security systems for our shared infrastructure-an infrastructure on which the national economy and the national security both depend.

John Hamre mentioned weapons of mass destruction and the threat that they could pose to the United States. I have taken a lot of criticism lately for urging the administration and Congress to spend more money to help us prepare for a WMD threat here in the United States. Some critics claim that there is no threat; that such an attack has never happened. They note that while an attack may have happened on the Tokyo subway, the cult responsible was so inept that the event never amounted to much. They have argued that I am exaggerating the threat and planning to spend a lot of money because people are scared.

As John pointed out, however, you have to [put in the infrastructure for defense] before the war, just as we did in World War II. It is too late after WMDs have been used in a terrorist attack to start wishing for a vaccine. You cannot develop a new vaccine in a year, three years, or even five years. The reality is that the threat may be more serious than we once thought. For example, we know that the Soviet Union before its collapse was experimenting with recombinant DNA techniques to take Biological Warfare (BW) agents and combine them with other organisms. This would make it possible to take airborne diseases and merge them with viruses like Ebola, which can cause death in two or three days. We do not know where all of that technology went. We have a pretty good handle on Soviet nuclear materials, but we do not know where all of the Soviet BW technology has gone.

What is more, all of the seven states that sponsor terrorism have some BW or Chemical Warfare (CW) program. These states have assisted terrorist groups with training, equipment, and money in the past, and it is unreasonable to think that they will not support them with BW or CW weapons in the future. Aum Shinrikyo's alleged failure in the use of nerve gas in the Tokyo subway is no insurance against a terrorist group developing its own lethal antigen or buying one from any of the 23 countries that have BW or CW weapons.

The challenge in this instance is not working with the private sector, as it is in the realm of cyber security, but rather working with state and local governments, who are the first level of response, and with the scientific and medical community, who will develop medicines and vaccines to address these threats.

The security of the U.S. border underlies all of these threats. We had some very interesting discussions with the Canadians in January following the incidents in December wherein several individuals sought to cross our border with bombs. We told the Canadians that they have to understand that if we are going to facilitate trade across the border-if we are just going to wave all those eighteen-wheelers across every morning-we have to have a common border. In short, we must have a perimeter defense around a homeland that includes Canada. We must have the same standards for asylum seekers and visa requirements. The Canadians were relieved to hear that we were willing to cooperate on creating a joint perimeter defense to reduce the possibility of terrorists and WMDs entering into North America.

Effectively guarding the border is a formidable challenge. Although we have tripled the size of the border patrol in the last eight years, we are also facilitating trade through NAFTA and the WTO. The result is that very little customs inspection occurs, and people and materials still get through. How do we solve the tension between trade facilitation and the movement of people, which we want, and the reality that this may mean very little inspection? Moreover, how do we encourage people to come and study in the United States, which is a great source of income for our universities, and yet address the fact that we don't really know much about who these foreign students are, where they are located, and what they are here to study? The current laws and procedures are such that we really do not know the answers to these questions. These are issues that must all be considered as part of Homeland Defense.

We have started to address a number of these concerns. We have some programs that are pretty far along and others that are just beginning. None of these issues, however, will be solved easily in the next few years. It is neither too late nor too early, therefore, for this group to address them. We look forward to providing what answers we may have, and to receiving your advice and counsel.

**COLLINS:** Our next speaker will be Representative Norman Dicks from the great state of Washington.

**DICKS:** I would like to thank John Hamre for staying in public service and for addressing this important issue, and I am glad that CSIS is taking it on. I compliment John for the work that he did over at DOD, where he took some serious steps toward dealing with the threat posed by cyberterrorism. I would also like to recognize Dick Clarke for his work on the president's commission. Addressing Homeland Defense directly and squarely is important to the country's security, and I think Dick is doing a fine job.

National Missile Defense (NMD) is the major issue we face in Congress this year. Some testing still must be done on the system, and there are several decisions that will have to be made. If we can get it to work, this system will go a long way toward addressing the concerns raised by the Rumsfeld panel report regarding the threat from rouge states. The last test failed, however, and there is still some question in my mind as a member of the Defense Appropriations Subcommittee

as to whether we can actually do this. Frankly, when you look at these defense-related issues, theatre missile defense (TMD) and the ability to protect our troops when we deploy them is equally important and may be more feasible in the short term.

There is a consensus in Congress to move forward on a first phase NMD system, assuming it works and assuming we can deal with the problems posed by our allies and the Russians. Working with the new Putin Administration in Russia to negotiate an agreement that alters but does not abrogate the 1972 ABM Treaty will be the major challenge for this Administration in the next few months. I am not in agreement with my former colleague Richard Pearle, who argues that we should simply abrogate the treaty. Such an error in judgement would cause serious problems not only with the Russians, but with our own allies as well-the majority of whom do not feel that they have been properly consulted on this issue. In the meantime, a great deal of work must be done up here on Capitol Hill to lay the foundation for any future agreement, which may include a START III nuclear armaments reduction pact. Time is running out for this administration to put all of this together. This is a serious challenge and one that must be addressed.

Terrorism is the second asymmetrical threat to the American homeland. This was made especially clear to me when some very alert U.S. customs agents in my home district, Port Angeles, Washington, seized a car carrying potential fertilizer weapons. That was good fortune on our part, but it demonstrates that we need to take a closer look at these issues. We need to be concerned not only about protecting the country's borders, but also with having good intelligence. Our intelligence efforts are crucial in being able to anticipate attacks. Closer coordination between the counterterrorism center at the CIA and the counterterrorism division at the FBI is needed in order to have both the necessary information and the ability to act on it.

We also need clear response strategies in the event that we are attacked. We in Congress have been briefed about the disruption tactics used against Osama bin Laden. Those tactics are indicative of the sort of operations that may be needed. In the future, the House and Senate intelligence committees must work with the administration on the various related counterterrorism and terrorism response operations, be they covert or overt.

On cybersecurity, numerous studies have indicated that our country is extremely vulnerable. It is not just the government. It is also the utilities, the banking industry, and our economy. Frankly, I am not all that worried about the so-called rogue states launching a direct military attack. I still believe the deterrent effect of our strategic nuclear triad, would cause anyone to pause. If I were in their shoes, however, I might try to attack the United States through terrorism and cyber warfare-through means that are not as readily identifiable.

When you launch a missile, for example, our satellites know about it in two or three seconds. There is direct evidence as to where that attack is coming from. In the case of the World Trade Center bombing in New York City, however, you cannot determine as readily where the perpetrators are from and who is supporting them. There is uncertainty there. Those are areas we need to focus on. We are going forward with NMD, but the other issues are just as important and need just as much attention.

We are spending a significant amount of money on these counterterrorism efforts, and we need to continue to be focused on that. I would just say on behalf of the members of Congress that there is a lot of concern about these issues and a willingness to work with the administration in addressing them. I think the challenge for CSIS is to look at all these various areas and give the country a good solid report that deals with them.

I am happy to end on that note. I look forward to being a member of this advisory group, and I am glad the President and Mr. Clarke are taking leadership on this issue. Their efforts will have a lot of support on Capitol Hill. It normally takes us fifteen to twenty years to build a new weapons

system. We can do much more in a shorter length of time, but we need the leadership and commitment to do it.

**HAMRE:** Would Governor Whitman like to say something? We have yet to hear about these issues from a governor's perspective.

**GOV. CHRISTINE TODD WHITMAN:** I would be happy to add some of that perspective to this conversation, particularly with regard to WMDs and civilian defense. As you know, every governor is the commander-in-chief of their state's National Guard, and the Guard is the first line for the states in responding to emergencies. The Guard's mission has changed over the last few years, however, and they have been called on to do some things and undertake some missions that had not normally been within their purview.

The question that I still have is how command responsibility will fall in the event of a terrorist attack. If the president calls up the National Guard, his authority supercedes that of any governor. For actual deployment, however, it will be the people on the ground in a state that will know where their people are, and where the greatest likelihood of mass impact from an attack would be. We are also the ones who will be responsible for any evacuations that may have to take place. Moreover, states will need to control or have a large role in controlling the communications system that will be critical to managing the aftermath of any WMD event.

I do not expect that the states are going to be paramount in prevention. I doubt that we will reach that stage, as that is not our role. Our role is going to be very important, however, when it comes to managing any of these issues at the state and local level. We have been talking about the new WMD Civilian Defense units. The State of New Jersey, the most densely populated state in the Union, does not have one. We will be protected by the centers in Pennsylvania and New York, neither of which is located near the border with New Jersey. I am very concerned that it is not clear who will respond and who will decide the priorities for my state and the eight million citizens who reside there, should there be an attack.

What is true for New Jersey is equally true on the West Coast, where you have some high population concentrations, as well as large rural areas. How do we manage deployments? Who has priority? Who has control? What will be the role of the governors and the local governments? As is true so often for so many of these things, it comes back to the governors to manage the fallout, literally or figuratively, of any kind of terrorist attack that may occur. We are the ones, along with our mayors and local government officials, who must actually deal with people. It is fine to deal with the theory, and we want to be part of that process, but ultimately we are the ones who are responsible for dealing with the people. These are issues that I believe this group must start to address.

What we are focusing on is the question of how to protect the population. Protecting our information technology and communications infrastructure is particularly important in that respect. Although it had weakened by the time it reached us last year, Hurricane Floyd still managed to knock out the telecommunications system in New Jersey for the better part of a day. The result could have been disastrous. Our emergency personnel could not talk to one another. The State Police had to set up special mobile units to be able to communicate with local police. Citizens could not get through on the phone lines. If that sort of thing can happen in a state that where Bell Atlantic, AT&T, and Lucent Technology are headquartered, it can happen anywhere. This is a very serious issue, and we have taken steps to rectify that problem. Without effective communications, no government has the ability to direct people to relieve problems as they occur.

I am looking forward to being part of this group and bringing my perspective to the table. I also look forward to working with the other governors who are going to be a part of this initiative. Being

here and having a voice is important. A lot of what the next Administration will decide will have to be implemented through the states, and that is where my colleagues and I have the expertise.

**QUESTION:** Do you think that what has happened with the National Guard in recent years has affected their ability to address these tasks?

**WHITMAN:** We can argue over what has happened as far as the Guard's ability to maintain their level of readiness and training. Financial problems have upset everyone's efforts to keep the training up to the level we would like. It is certainly less than what would be optimal. Regardless, I still think that the National Guard is the most appropriate means for responding to WMD attacks. You cannot deploy the U.S. military quickly enough for this task. You have a National Guard in place in each of the states, however, and they are certainly capable of fulfilling this sort of mission. It is going to involve some retraining, however. The National Guard needs to know what to do with someone who has been attacked with some sort of chemical or biological weapon. Do victims need to be isolated? How do you isolate them? Triage decisions will need to be made immediately, and at this point we are not fully prepared to make them. The Guard is a resource that must not be overlooked. That is why the WMD Civil Support Teams (CST) are so important. We in New Jersey need to be involved, even if we do not have such a unit located in our state.

**HAMRE:** This gets to some interesting federalism issues. If you federalize the National Guard, for example, you are now subject to posse comitatus and you cannot conduct police activity. If the Guard stays under state authority, they can continue to exercise police authority but will remain outside the federal military command and control system. Hence, there is a question as to who should become the Commander-in-Chief in the event of a very serious incident. Can I get your reaction to this?

**WHITMAN:** If the president calls up the National Guard, obviously his authority supercedes that of any governor. Our New Jersey forces have been deployed around the world in a series of non-traditional roles. If there is a threat to national security, I know of no governor who would want to be in a position of having to make all of the determinations. We will be happy to take directions from the experts in Washington, so long as we can issue the necessary orders through our adjutants general in order to direct our forces on the ground. This will allow the Guard to maintain their policing authority. Effective command and control need not preclude these policing powers.

**CLARKE:** This also depends on the incident in question and the advice that the president gets from the governor involved. The National Guard is the same group, regardless of whether it is federalized or working under a governor. They already know what to do and who to call. They already exist within the broader military framework.

John's question is really about policing authority. We use the term posse comitatus a lot, and it is important that we understand what it means. It is a post-Civil War law that prevents the U.S. military from exercising police-like powers, such as arresting people and using force within the United States against American citizens. The president, in consultation with a governor, can waive this law at a moment's notice, as it was during the Atlanta prison riots nearly a decade ago. If the decision is made to waive posse comitatus, it can be done rapidly. Moreover, I do not think it is an issue that is central to the use of the National Guard. We should keep in mind the fact that arresting people and using forces is not what the National Guard is likely to do in a WMD crisis. Most of what we want out of the Guard is medical support.

**HAMRE:** I raised this issue only as an example of the complex issues these questions raise. Mechanically, it is not hard to waive this law. It is an enormous step politically, however, to tell the public that we are going to waive posse comitatus in a flash. This is a problem for the American public, be it those on the right, who fear black helicopters swooping in, or those on the left, who

fear violations of civil liberties. Let me quickly turn to Representative Weldon. Thank you so much for coming sir, we are delighted to have you here.

**REP. CURT WELDON:** It is a pleasure to be here, and to welcome John to CSIS. He is one person who has the respect of everyone in Congress. The administration is going to miss him and his expertise sorely.

I appreciate the opportunity to share my feelings on Homeland Defense. The biggest issues that I face as chairman of the Research Committee on Security are missile proliferation, WMD terrorism, and the issues involving information dominance and protecting our information systems. We are aggressively engaged on those issues, and I am not going to discuss them further today.

What I would like to discuss is the question of who is the first responder to Homeland Defense threats. It is neither the military, nor the civil defense community, nor the senior bureaucrats. It is the 1.2 million men and women who serve in the 32,000 organized fire and emergency medical system (EMS) departments across this country. As a former fire chief myself, allow me to note that these professionals have largely felt ignored by a federal bureaucracy that is now starting to tell them how to do their job. In fact, the federal government recently issued instructions on how to deal with a hazardous materials incident (HAZMAT) despite the fact that the Fire and EMS community has responded to every HAZMAT incident at every chemical and oil refinery in the country for the last 250 years. They already have the necessary practical experience.

We must engage this community in a way that it has not been engaged before. That is difficult, because 85 percent of these first responders are volunteers. The federal government does not know how to work well with volunteers. We do not innately understand the concept of people doing things simply because they believe it is best for their community. The worst thing we could do as a nation, however, is to think that we are going to reinvent the manner in which we respond to disasters on the local level. I can think of every disaster we have had in the last five years: hurricanes Andrew and Floyd, the bombing in Oklahoma. I was there observing a lot of these events, a day or two after the incident. In every one of those incidents the command decisions made in the first five to ten minutes ultimately affected the severity of those incidents with respect to the loss of life and property.

We need to engage the Fire and EMS community in a very positive and proactive way. They are our domestic defenders. Yes, there is an important role for the military, for the Marine Corps' Chemical/Biological Incident Response Force (CBIRF), for the training and resources available through our National Guard and Reserve forces. There is also a role for the federal agency network. The first responder is not going to change, however. It will continue to be the Fire and EMS leadership at the grassroots level, be they paid or volunteer personnel.

First responders face some serious challenges, chief among them the current state of our emergency communications system. When Chief Morris, the chief of a very competent paid department in Oklahoma City arrived on the scene of the Murrah Federal Building bombing five years ago, the communications system was so uncoordinated that he could not talk to the police, the volunteer fire departments that were arriving to help him, or the federal agencies that responded to the attack. When I asked him if he was better of a year later, he said that the communications situation was exactly the same. In fact, we still have no coordination of our emergency communications system in America.

Let me give you another example. After the 1993 World Trade Center bombing then Fire Commissioner Howard Safir told me that the biggest problem in New York City was a lack of coordination and communication. During the crisis, Commissioner Safir had TV stations broadcasting messages instructing the people trapped in the upper stories of the World Trade

Center building to knock out windows. There was no other way to communicate with those people in those complexes. Clearly, we must develop some sort of integrated communications system for first responders.

Communications, however, are not the only challenge. DOD and Department of Justice (DOJ) training ultimately does little good when localities cannot afford to maintain their equipment. We are giving 125 cities across America chemical and biological warfare gear at a time when they cannot even buy boots for their firefighters. A few years ago Washington, DC, had only one aerial truck for the entire city. Now we expect the DCFD to have an aggressive HAZMAT unit capable of responding to local incidents.

We spend \$3 billion a year at the federal level for local law enforcement and practically nothing to help equip our first responders in terms of fire and life safety. Even though these must remain state and local responsibilities, this funding disparity is outrageous. Training must go hand-in-hand with adequate communications and equipment. Thankfully, there has been some progress on these issues. Last year in the House of Representatives we put \$100 million toward supporting local responders-the first such effort in our nation's history.

I encourage and challenge you to consider the implications of your recommendations for the first responder community. If you do not, your solutions will not work. America has had this group of people working at a local level for over 250 years. First responders are already institutionalized, and they are waiting for someone at the federal level to provide the integration plan necessary to fully engage them in dealing with the disasters that America will continue to face. They are not going to go away. The community is politically astute, and is becoming more so.

Please keep these issues in mind as this task force moves forward. What you are doing is extremely important. Homeland Defense is a major issue right now for us. We in the Congress are engaged on this issue in an bipartisan way unlike any other in the fourteen years I have been here. We will be there to support your recommendations and conclusions.

**COLLINS:** Let's continue with our dialogue.

**CORDESMAN:** I would like to take a moment to raise some of the questions that have come out of the work I have done so far. John began by saying that there is no such thing as a unified field theory, and I agree with him. There is, however, such a thing as a unified field: money. One of the great challenges in this endeavor is trying to figure out who is spending what, and what they are trying to buy. As you look through federal budgets and federal programs, it is very difficult for anyone on the outside to get even a rough idea of where the money is going. There are many starts, but it is often very unclear what the end goal is intended to be. This is something that the panels will have to consider.

Another issue lies in this word "homeland." Clearly we must also consider the role of a strong foreign defense and the role of foreign counter terrorism. What role do deterrence and retaliation play in relation to Homeland Defense? These are not easy questions, and I do not know how you make the necessary compromises. In theory, however, that is what we are supposed to do.

I am also worried that groups conducting individual studies in this field have outdated research and development concepts, some of which I am now seeing for the third time. Many of the technologies in question were being touted for other purposes back when John and I were working on the Senate staff. What is more, many of these groups do not have a clear deployment plan. There is almost no clear analysis of the military cost of defeating or circumventing some of these proposed systems-a key test of their relevance for national defense.

One of the other things that I find in looking at the terrorism issue is uncertain information regarding the warheads or agents that could be employed in a WMD strike. I am deeply disturbed by the kind of biological lethality data that I currently see. I can find neither its source, nor evidence that these models have been thoroughly re-examined. The broad range of unsubstantiated opinions among experts regarding a given weapon's lethality and the ease of manufacture leaves me almost completely puzzled as to what we are really talking about. Hence, a central question for all of us involved in this initiative is the balance between offensive and defensive capabilities. If you cannot measure these relationships, it is impossible to determine what threats really exist, and what sort of response is required.

The last issue that keeps coming up again and again in my investigations into information warfare is the difference between external, deliberate threats and the threat posed by hackers. People talk about the new economy. To what extent will information warfare be a cost to this new economy? If that is a cost, then who should pay for defense? Is it a matter of federal incentives or a matter of corporate liability? And if we are dependent on rented systems, who is responsible for defending them? Should corporate officers be criminally liable for the issue of information warfare? These are just a few of the many issues that go beyond politics and get into technical problems that we must all begin to deal with.

**COLLINS:** General Meyer?

**GEN. (RET.) EDWARD C. MEYER:** Could we talk about the national borders? We have devoted a lot of resources to the border patrol during the last eight years while trying to facilitate trade at the same time. Our current contraband interception rate is probably around one percent of the containers entering the United States.

Two questions logically follow. The first is whether you can develop better resources so that our inspections are intelligence-acute rather than random. The second question is whether we can use some of the military projects that we have had under development for some time to scan for drugs, WMD-related materials, and explosives. The military application of this technology has shown this to be possible.

**CLARKE:** Both borders are a source of concern. It is far more difficult for people to cross the Mexican border than the Canadian border, however, as we have many more resources deployed there. I think you have to look at both of these borders and our third border, the Caribbean. That third border is essentially porous, be it with regard to an influx of either drugs or terrorists.

**ARNAUD DE BORCHGRAVE:** My question is also for Dick Clarke, and it regards the incident involving the interception two or three days ago of nuclear materials that was being brought across the Pakistani border. What are the implications of this incident for the security of nuclear materials from the former Soviet Union?

**CLARKE:** I think we have a good feel for the level of security at a number of Russian nuclear weapons sites. That was not true five or six years ago. What we do not have is a feel for the level of security at Russian BW or CW sites. Nor do we have a good feel for the location of BW and CW sites anywhere. We have tended in Homeland Defense policy planning to deal with CW and BW. That is our primary concern.

Only in the last few months have we really begun to look at nuclear threats. Most of us are old enough to have grown up with civil defense training in the classroom, and most of the institutional memory in the federal government from that era is still relevant today. We do need to take a moment to reconsider some of the modern implications of such a nuclear attack, however.

Moreover, when we think about nuclear materials, we must remember that Russia is not the only country that has them. We have to plan our Homeland Defense based on threats that are three to ten years in the future. Pakistan is problematical in this regard. This situation is clearly an important security threat. But what other nuclear states will there be three to five years from now? I do not think we can take comfort in knowing where the Russian nuclear materials are and the extent to which they are properly guarded. There are other nuclear weapons out there, and there are going to be more countries with more of these weapons. We need to broaden our perspective in this respect.

**COLLINS:** Dov Zakheim?

**DOV ZAKHEIM:** You talked about detection and prevention along the southern border. What about training? In my mind, training is one of our most important assets. To what extent are we training the border patrol to look for the kind of people that pose a threat?

**MEYER:** There are training programs for some of the customs and immigration officials on the border. The real problem is with recruiting and retaining Border Patrol personnel.

**COLLINS:** Frank Cilluffo?

**FRANK CILLUFFO:** I have two quick questions. The first is for Dick Clarke and the second is for Representative Weldon.

With regard to information assurance, I agree that a lot of the emphasis has been placed recently on capturing perpetrators rather than keeping them out in the first place. We need to emphasize that information assurance entails far more than just a "beep and sweep". Rather, it is a policy, people and technology issue. Underpinning that dedication and awareness is the question of sound leadership. Who should be in charge of the information assurance assets outside the DOD and intelligence community?

And for Congressman Weldon, if you had a laundry list of the top five things that the first responder community should have to better manage the consequences of a WMD attack, what would those be? What concerns you most?

**CLARKE:** There are two issues involved with information assurance. The first is the question of who is in charge of outreach to the private sector. The Commerce Department, has done a tremendous job in this area by organizing a partnership for critical information security that includes over 150 companies, including a good number of Fortune 500 CEOs.

The second issue is a question of how you organize the federal government to ensure the security of federal institutions outside the defense and intelligence community, I think the United States needs an Chief Information Officer (CIO). The law says that every Department needs to have a CIO. Nearly every major company has a CIO. The federal government, however, does not yet have someone with the authority to shut down systems, someone who can go into a department or agency such as the FAA, NASA or the IRS and tell them that their Information Technology (IT) section is in receivership. If we do not have that sort of information leadership, we are never going to reach our goals in terms of protecting departments that have vital information in their systems.

We recently started looking at the departments and agencies to see who really has critical information on their computer systems. The results surprised us; every department has critical information. For example, it had not occurred to us that the Department of Commerce runs a satellite system for tracking vehicles, including nuclear weapons vehicles. Nor did we think about the computers at the National Weather Service. The reality is that we must be secure at every

level in every department, right up to the Secretary's office. The trouble is that outside of the defense and intelligence community, many departments remain more concerned with their traditional mission and do not see information security as an essential component thereof. They are not going to get it right on their own.

**CILLUFFO:** I think we can agree that this is an intolerable position.

**PARTICIPANT:** Let me add one more thought to this discussion. If I were to look at this country, I would say that our agriculture system and our animal husbandry system is probably more vulnerable than anything else, as it tends to be centralized in various locations.

**PARTICIPANT:** Senator Lugar agrees with you, and as a result the government is taking a new look at biological threats to the agricultural sector.

**WELDON:** I would first like to add to Frank's comment about the information assurance issues. I am convinced that our 28 separate agencies are still stove-piped, and that each has classified systems or networks that should be integrated. Hence, the data in that system are not adequately protected or coordinated. If you are going to conduct a broad-based data profiling to understand the possible implications of a terrorist attack, then the federal agencies must monitor the relevant classified and unclassified data in a cooperative way. The CIA and FBI are now moving in that direction. In his former position, John Hamre suggest that DOD should fund these efforts, and I agree with that. This has to be managed at the White House level. Moreover, we need to create a center involving those agencies with systems that can bring data to bear that can be analyzed, assessed and used both to predict events. The ability to use America's capability for information dominance to defeat those individuals who want to take down our systems will be crucial to the future success of Homeland Defense.

I have several comments regarding Frank Cilluffo's second question. First we need an integrated Homeland Defense response plan. There is none. And if we think there is, it is only the bureaucracy in Washington talking. There are thousands of local personnel across America responding to crises every hour of every day that are not yet integrated. They feel left out. What is more, our focus has been on working with Fire and EMS people in larger cities. These are all paid personnel. The bulk of the risk in America is not just in our cities, and approximately 85 percent of the available first responders across the nation are volunteers. If we do not reach out to them and make them full-fledged players in this process, we will fail. Ultimately, they will be the ones making tough decisions in the first five to ten minutes of a crisis.

The second key issue is the communications system. We need to look at the frequency spectrum availability and find a way to integrate emergency frequencies among federal, state and local agencies. That sort of integration does not exist today, and it must take place.

The third issue involves resources. We are asking first responders to make a determination in instances when they may lack the tools to assess whether the danger is from a biological agent or something else. That will require new tools and new training. If first responders do not have those assets and that information, they could inadvertently compound the problem in dangerous ways. Some of our cities are beginning to get some of the necessary training and resources from the Department of Justice. These assistance programs must not become an unfunded mandate, however. Training first responders once and then leaving them on their own is not the answer, especially given the way most city budgets are.

Fourth, integrating some of the defense technology currently under development for scrutinizing a battlefield should be considered. GPS positioning equipment and aerial surveillance have clear applications for Homeland Defense. We do not yet have an aggressive strategy to make this kind of technology available to civilians. If we are going to build and fund these great systems, we

need to consider their applications not only on the battlefield but here at home. Civilian disasters cost us on average one hundred lives each year. And yet, we don't put the same focus on protecting those individuals as we do on protecting our military forces.

**COLLINS:** James Kitfield from the *National Journal*.

**JAMES KITFIELD:** I do not want to make this a bureaucracy-building exercise, but is there a specific commander-in-chief (CINC) or staff with a budget that would be looking at all of these things?

**HAMRE:** The glib answer is that we have a CINC, and that is the President of the United States. Disasters like this will require one authoritative voice, and that must be the President. You are right to ask the question about a planning staff, however. One of the reasons that DOD has had a vacuum in this particular is because we have not had Homeland Defense under one particular staff. This is due in part to the fact that there are a lot of Americans who are deeply apprehensive about the notion of a "CINC-America." We have to be very careful about this. The most important thing for us to realize is that we must get ready without doing so in a manner that threatens public confidence. There are a lot of citizens on both the left and the right who are worried about the implications of Homeland Defense for their civil liberties.

**KITFIELD:** It would probably require a civilian organization. We already have the FBI, FEMA, and the local responders. What I mean by CINC, however, is someone who thinks only about these issues and has the necessary staff and resources to set policy.

**HAMRE:** DOD's contribution to such a staff is the Joint Task Force for Civil Support. That task force must work in partnership with the FBI and the rest of the federal government. Frankly the most actively interested in these issues is in the law enforcement community. That presents something of a problem, however, because while the federal response to local disasters revolves around FEMA, FEMA personnel have not been as involved in thinking about Homeland Defense.

**COLLINS:** Once again, thank you all for coming. The Senior Advisory Group will meet again for breakfast somewhere on Capitol Hill on July 11. Our study group leaders will be the featured speakers for that event.

These proceedings were prepared by Chris Swift of the Center for Strategic and International Studies.

"Defending America: Redefining the Concept of Homeland Defense"

First Senior Advisory Group Meeting

April 5th, 2000

8:00 a.m. - 10:00 a.m.

Dirksen Senate Office Building, Room SDG-11

Participants

The Senior Advisory Group (SAG)

Pamela B. Berkowsky\*\*

Assistant Chief of Staff to the Secretary of Defense

L. Paul Bremer

Managing Director

Kissinger Associates, Inc.

David Chu  
Vice President and Director, Arroyo Center  
The RAND Corporation

Richard Clarke\*  
Special Assistant to the President  
National Security Council

The Honorable Max Cleland  
United States Senate

Ruth A. David  
President and CEO  
Anser Analytic Services

The Honorable Norman Dicks  
U.S. House of Representatives

GEN Wayne A. Downing, USA (Ret.)

Mark Esper  
Professional Staff Member  
Senate Committee on Government Affairs  
(for Sen. Fred Thompson)

Neil J. Gallagher\*  
Assistant Director  
National Security Affairs Division  
Federal Bureau of Investigation

Stephen J. Hadley  
Partner  
Shea & Gardner

John J. Hamre  
President and CEO  
CSIS  
(Ex officio member)

Edmund J. Hull  
Principal Deputy Coordinator for Counterterrorism  
Department of State  
(for Michael Sheehan\*)

Sir Laurence W. Martin  
Arleigh A. Burke Chair in Strategy  
CSIS

David McCurdy  
President  
Electronic Industries Alliance

Alan McCurry  
Military Legislative Assistant  
Senator Pat Roberts  
(for Sen. Pat Roberts)

GEN Edward C. Meyer, USA (Ret.)  
Chairman  
Mitretek Systems Inc.

Mary O'Brien  
Legislative Fellow  
Representative Ike Skelton  
(for Rep. Ike Skelton)

Kevin O'Prey  
DFI International, Inc.  
(for Barry Blechman)

The Honorable Charles S. Robb  
United States Senate

The Honorable Curtis Weldon  
U.S. House of Representatives

The Honorable Christine T. Whitman  
Governor  
State of New Jersey

R. James Woolsey  
Senior Partner  
Shea & Gardner

Dov S. Zakheim  
CEO  
System Planning Corporation International

Philip A. Odeen  
Vice President, Operations  
TRW

\* Advisor to the SAG \*\*Guest of the SAG and DOD point of contact

#### Other Participants

Gabrielle Bowdoin  
Research Associate  
International Security Program  
CSIS

Arnaud de Borchgrave  
Senior Advisor and Co-Director, Transnational Threats Initiative  
CSIS

Grey Burkhart  
Publisher  
United Press International

Joseph J. Collins  
Senior Fellow and Project Director, Homeland Defense  
CSIS

Anthony H. Cordesman  
Senior Fellow for Strategic Assessment and Co-Director, Middle East Program  
CSIS

Frank J. Cilluffo  
Senior Policy Analyst and Deputy Director, Transnational Threats Initiative  
CSIS

William B. Garrison, Jr.  
Director, International Communications Program  
CSIS

Kelly Glazier  
Aide to Governor Whitman

Daniel Gouré  
Deputy Director, International Security Program  
CSIS

Andrew Hunter  
Legislative Assistant for Defense Issues  
Rep. Norman D. Dicks

Bill Johnstone  
Senior Policy Advisor  
Office of Senator Max Cleland

James Kitfield  
National Journal

Alexander T.J. Lennon  
Editor-in-Chief  
The Washington Quarterly  
CSIS

Mark Montgomery  
Director, Transnational Threats  
National Security Council

H.K. Park  
Office of the Secretary of Defense

Susan Spencer  
Director, Washington Office  
State of New Jersey

Bill Sutey  
Legislative Assistant for National Security Affairs,  
Office of Senator Charles Robb

M. Jon Vondracek  
Vice President for External Relations  
CSIS

Sue Yang  
Associate Director of External Relations  
CSIS