

Proceedings of the September 12th 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, Chair: These meetings are like a chess game, so I am going to start with a safe move and call on my boss to say a few words.

JOHN HAMRE, President of CSIS: I am going to be very brief because we want to get into the content of our meeting this morning. First, thank you all for being here. This is an enormously difficult time of year, and it is wonderful that you were all able to come. I would also like to take this opportunity to thank Senator Roberts for doing something that has become all too rare in Congress: that is, taking on an issue for which there are no personal or political gain because it is important for the country.

As you all know, Senator Roberts has gone out of his way to create a subcommittee to focus on the Homeland Defense issue, and in so doing has brought more attention, creativity, and energy to this issue than anyone else in Congress. It is that kind of leadership that has made a difference historically and ensured that America was properly prepared to face the challenges ahead. On behalf of everyone here, thank you again for your leadership.

Let me turn it over to you sir, as we are eager to hear your remarks this morning.

SENATOR PAT ROBERTSON: Floyd Spence once said that "many are called, but few are chosen." We certainly have the chosen few here in this room. Thank you for the privilege of being with you all today. I must say that I have never seen John Hamre so relaxed, so tan, so rested and so ready.

I would like to give you all a pitch for something before I get in to my remarks. Some of us in the Congress have been privileged to serve on the Commission on America's National Interest, which has been organized by former NATO Ambassador and Assistant Secretary of Defense Bob Ellsworth. The Commission involves Harvard University's Center for Science and International Affairs, as well as the Nixon Center and the RAND Corporation. I would commend both this commission and its recently published report to you.

I am honored to host the CSIS Senior Advisory Group this morning. This group's work is vital, particularly because it provides a critical, unbiased look at terrorism--one of the most serious threats facing this country. As you all know, terrorism can come in any one of several possible forms: via biological, chemical, or nuclear weapons, and even via the Internet through cyber attacks. Another possible method includes a ballistic missile strike. Regardless of the source and method, however, the consequences of terrorism pose the same threat to our nation.

As John Hamre has indicated, I have the privilege of chairing an outfit that we in Congress call the Emerging Threats and Capabilities Subcommittee. This effort is led largely by Armed Services Committee Chairman Warner and Senator Joe Lieberman. The subcommittee has been

operating in both sessions, and I expect that the House will establish something comparable in the next Congress.

I have frequently asked the many experts that have come before our subcommittee what it is that keeps them up at night. In most cases, the answers fall into two basic groups. The first is the danger posed by cyber-terrorism against the economy. The second is the possibility of biological warfare--an issue we have heard so much about.

John said that there is not much of a political upside to these issues. That may be true, but there are an awful lot of folks--from civic groups to Rotary meetings to the League of Women Voters--who worry about these issues once they are brought to their attention. Our goal is not to scare people to death, but rather to inform them of the threats that do exist and present our proposals as to what should be done. It may get a little scary, but I cannot tell you how many people have spoken with me and expressed gratitude that someone is actively involved with these issues. This gives me some degree of confidence that the public is increasingly aware of the problem.

One of the issues we are addressing is the relative ease with which a small group of dedicated terrorists, be they state sponsored, independent, or just a group of wackos, could bring massive casualties and economic chaos to America's doorstep. We have many challenges ahead of us. I think we are all well aware of the report card issued by Representative Steve Horn and the Government Reform and Oversight Committee. His critical review is helpful. There is nothing wrong with beating up on the alphabet soup of agencies we have in this town if we do so in a responsible way--a way that directs attention to the appropriate officials as well as the appropriators responsible for their oversight.

Representative Horn's report was quite revealing. The reality is that we are not prepared at the federal, state, or local level to respond to the consequences of a terrorist attack--at least to the degree that we think we should. There are many unanswered questions regarding the impact of federal action on civil liberties and jurisdictional authority, as well as the Department of Defense's role in a catastrophic domestic event. Nor do we know how best to pursue proper civil defense education without scaring the general population. What's more, there are many unanswered questions regarding our ability to defend against a cyber attack at the national level without violating the online industry's privacy concerns. We have also had trouble gaining the confidence of those in private industry whose support is crucial in developing a workable defense strategy--a strategy that is in everyone's interests.

We should also note that America's medical community lacks the capacity at the local level to deal with the likely fallout from an attack with a Weapon of Mass Destruction (WMD), be it biological, chemical, nuclear, or radiological. We are making progress in this regard, however. Kansas City, for example, is now making a determined effort to encourage collaboration among the many excellent medical centers we have there. As we reassess our capabilities in the medical field, it is important that we determine how well these institutions and others are truly prepared to deal with consequence management.

I am not going to list all of our other deficiencies. You are well aware of them. CSIS has taken the lead in bringing outstanding expertise to address these issues. It is clear to me that you are deep thinkers capable of analyzing issues and proposing solutions. It is a tremendous challenge, but we will get the job done. Thank you for being a part of the team.

JOSEPH COLLINS: Thank you, Senator Roberts, for your comments and encouragement. Let me say a few words about the organization of our project, as it is quite complicated. Ours is a three-part initiative. The first part entailed voluminous analysis by CSIS Burke Chair Tony Cordesman. The results of his broad study are available on our web site. The second part of our effort is organized into four ongoing working groups: one on missile defense led by Dr. Dan

Gouré, another on cyber threats led by Arnaud de Borchgrave, a third on Chemical, Biological, Radiological and Nuclear (CBRN) weapons led by Frank Cilluffo, and a fourth group on policy integration led by myself. These four groups will publish their reports this year.

Our goal today is to preview some of the central issues that have arisen in our meetings and petition you for your opinions on them. We are not here to brief you on our conclusions, but rather to establish a dialogue. Following this dialogue, we plan to interview many of the Senior Advisory Group's members in order to augment our study. We will then meet in February next year to present our findings.

Let me take this opportunity to talk about organization--an issue that has arisen repeatedly in my working group. There was little happening in the field of homeland defense five years ago. Today, there is furious activity, with approximately \$10 billion each year allocated for new plans and programs. The only way to address the challenges posed by the haphazard approach to homeland defense is with better organization. To this end, we have studied a number of different ideas. The first of these is to create a supercoordinator and a national council for homeland defense. The second was to have a new Deputy Attorney General who would be responsible for these issues. The third proposal was to establish a new Department and cabinet position--a model with some clear limitations given the number of Departments currently involved in these matters.

The vast majority of those participants in my working group and at CSIS think that we ought to make better use of the Vice President. The President would make the Vice President responsible for most aspects of homeland defense. In performing these duties, the Vice President would be supported by an Emergency Planning Staff (EPS) drawn from the office of what is now the office of the National Coordinator for Homeland Defense, as well as from selected departments and agencies.

Under our proposal, the Vice President would also chair a National Homeland Defense Emergency Planning Council, which would include representatives from all departments, agencies, states, and territories. Private sector organizations would also be invited to participate in this nationwide organization. The Council would meet twice annually, once at the principal level (the Vice President, Governors, etc.) and once at some subordinate level to be determined. The head of the Federal Emergency Management Agency (FEMA) or the National Coordinator would be the Council's Vice Chairman. The Vice President and the National Coordinator, in turn, exercise supervisory authority over FEMA.

Under our plan, the Vice President and his Emergency Planning Staff would perform a number of tasks including, but not limited to, preparing annual reports, and evaluating our ability to prevent, deter, and respond to threats against the homeland. They would also coordinate national plans for critical infrastructure protection and combating domestic terrorism. They would assess the adequacy of agency budgets. In addition, they would develop and evaluate a series of exercises at the federal, state and local level.

In addition to supervising all aspect of emergency planning for the government, we believe that these new structures would not necessitate major revisions in the Department of State and Department of Justice's respective roles in crisis response and consequence management. As I noted before, there would be some consolidation of offices and functions to support the EPS.

I will now ask each of my colleagues to speak for a few minutes. We will then have a discussion when they have finished.

DR. DAN GOURÉ: Two things are clear from the discussions both inside and outside government regarding missile defense. The first is that there is a growing need for some form of

national missile defense. The second is that a defense against a basic ballistic missile threat is indeed possible. Based on those facts, we should think of the period ensuing from the Clinton administration's decision to delay the decision on deployment as a window of opportunity. The fact is that we have a statutory agreement to deploy an effective missile defense as soon as possible. The question therefore is not whether we should deploy such a system, but rather how to establish the basis for a confident assessment that such a capability is at hand.

There are several issues that the next administration should pursue if we are to take advantage of this opportunity. First, we need to expand the development program in order to ensure that we can adequately judge the state of the systems and technology. One member of our working group argued that we ought to be launching a test vehicle every month given the importance of this issue. Second, Ballistic Missile Defense Office (BMDO) at the Department of Defense (DOD) ought to address the countermeasures issues, not only in terms of paper studies, but also through actual testing. This research must be done, if only so that our interceptors have multiple targets to assess.

I am a veteran of the Strategic Defense Initiative (SDI) countermeasure wars and have two points relevant on this subject. The first is that developing good countermeasures is very difficult. In fact, countermeasures may be beyond what countries like North Korea or Iran can produce. Truly effective countermeasures may make it impossible for missiles of the Taepo-Dong class to deliver a payload to the continental United States. Indeed, ignoring North Korean efforts to develop countermeasures may be a sensible policy, provided those efforts ultimately undercut the viability of their program.

Third, we need to reassess the question of non-ground based sensors, including the space-based infrared low system. There are two reasons to do this. First, space-based sensors make a real difference in dealing with the mid course targeting envisioned in our land-based defense strategy. Second, global sensing offers the opportunities associated with avoiding the need to build or upgrade land based sensors. One of the potential problems for an initial NMD deployment is finding allies willing to allow the presence of tracking sites on their territory. Space-based, global sensing would allow us to circumvent that problem.

These sensors, weapons, and command and control systems will come together sometime around the end of this decade, and we need a way to make this happen in a coordinated fashion. Yet, while we should continuously evaluate the options for the enhancement of a potential land-based system, those evaluations ought not to delay the current push for deployment. We have already had too many programs chasing too few dollars. Nor should we be sidetracked by the boost phase option, which suffers from a series of operational, technical, and even political shortfalls that prevent it from being a supplement to or an alternative for a land-based NMD system.

We must also accept the political reality that an effective defense, even against a limited threat, is impossible under the 1972 ABM Treaty. The question is therefore not whether or when to modify that treaty, but rather how. There are only three strategies. I support the "modify early but often" approach in which the United States would take incremental steps towards initial deployment. In my view, the treaty should focus on the adaptation of mutually-agreed arrangements, rather than sustaining an unworkable arrangement and its associated consultative mechanisms.

The alternative to this incremental approach is to abrogate the ABM Treaty altogether. An effective defense against the threats envisioned in the next twenty years will ultimately require several interceptor sites, a range of sensors, and the freedom to test and deploy both in four to five major areas. Those changes demand a new treaty. If we really want to move forward with missile defense, this might be the best option. We could then set a date for negotiations over future deployments, should they become necessary.

The third option, of course, is not to proceed--an option that is unlikely, given this administration's policies, intelligence assessments, and so forth.

Finally, we need to invest more money in this initiative. The current estimate for the overall program now before us is \$25 billion in spending up to 2007, with another \$48 billion out to 2026. We should plan for an addition \$10-12 billion in spending over the course of the next seven years in order to accommodate the need for expanded testing, development, and the possibility of an initial site deployment. Such deployment could take place at Grand Forks under the AMB Treaty's current terms.

This is not going to be cheap. We are currently envisioning a system that will cost between \$60 and \$70 billion for a single interceptor site, a figure that does not include the cost of enhancing our Theater Missile Defense (TMD) capabilities. I believe that a system deploying interceptors at two or three sites, built on global sensing capabilities, and augmented by an expanded TMD system, would cost around \$100 billion. That is only a first order estimate, however. The costs associated with defending U.S. territory, forces, and allies from an ever-expanding range of possible attacks bears further consideration.

ARNAUD DE BORCHGRAVE: I think the first conclusion one reaches in examining future cyber threats is that one month's crisis quickly becomes irrelevant the following month.

The Internet has lashed together the world's largest computers, and it will soon incorporate even the smallest. Nearly all of the world's major information technology (IT) companies--from Sweden, to Japan, to this country--are racing to adapt Ericsson's Bluetooth technology, which could extend the internet to almost every machine on earth capable of receiving a ten-meter radio signal. This form of remote-control means, ubiquitously, that computing has taken over the entire world. It also means a quantum leap for troublemaking in cyberspace.

I read two interesting article yesterday: one that gave the United States government a D- rating in terms of cyber security, and one that warned of the growing cyber threat to a wide range of critical government operations. I hope that this vulnerability will help push cyber security issues right to the top of our national security agenda.

From cyber extortion to cyber stock scams to cyber espionage and threats of cyber terrorism, we are woefully unprepared. There are now an estimated 50,000 piracies taking place on the World Wide Web, with thousands more being concocted all the time. What's more, there are about 30,000 hacking sites, 2,000 of which offer sophisticated programs for cracking passwords, software packages for writing viruses, and scripts for penetrating and disabling major networks. Information on how to conduct cyber attacks has become commonplace in just that last five years. Some of the computer engineers that we consulted predict viral outbreaks far worse than what we saw with the "I Love You" bug--a bug created by a student with only fifty lines of elementary computer code.

In this never-ending security battle in cyber space, we now find technology rapidly coming on stream that will displace passwords with retina, hand, face, voice, and fingerprint scans. This technology is not a panacea, however. The German Information Security Agency has determined that fingerprint scans can be tricked by applying layers of silicone to one's fingers, much the way it was done in the James Bond movie *Diamonds are Forever*.

After hearing from leading cyber security experts, and after studying many aspects of coming disruption technologies, our working group believes that the key to promoting cyber security lies in motivating the private sector to undertake preventive measures largely ignored by the marketplace. Although the federal government does not own the Internet's infrastructure, it can still create powerful incentives for the IT industry. The fact is that the federal government could

even mandate action by using the same mechanism employed during the Y2K emergency last year. That is, by requiring companies to report their compliance with established standards to the Securities and Exchange Commission (SEC).

Government incentives may also be structured through tax breaks that limit liability in much the same way as with the credit card industry. There is precedent for this. Government incentives actually encouraged credit card companies to invest in full-protection software and operating procedures to limit the use of stolen cards.

Similar steps can be taken to encourage the insurance industry to issue policies against cyber disruption. Working together, the government and private sector could establish a method of certifying the safety and effectiveness of online security products. We could establish a method for sharing government information with industry similar to the government-funded Computer Emergency Response Teams-a systems that has already been developed by IBM and others in order to deliver security services to the private sector. Government could also establish better risk management mechanisms for cyber inspection authorities based on insurance industry models for assessing risk before issuing policies. It could also explore new limited liability measures contingent upon certified steps for cyber protection initiatives.

The U.S. government must also begin to assess and take responsibility for extraordinary liability relief in case of a major catastrophe-be it a cyber Exxon Valdez, a cyber Oklahoma City, or even a cyber Pearl Harbor. Thankfully, there are precedents for the sort of extraordinary indemnification of commercial assets used by the government that may be destroyed by an act of war.

Finally, there is an extremely urgent need for government to institute a catch-up program for training specialists in information assurance. In 1999 there were only ten American doctoral students who selected this field as their specialty, versus hundreds of non-Americans. Increased student loans for specific technological institutions and targeted cyber-scholarships should be considered to close this gap. We would certainly appreciate any thoughts the you may have on this particular front.

FRANK CILLUFFO: I would like to remind you of our mission before reporting on our findings. Our mission was to identify programs on the CBRN front that have worked, to identify programs that have not been all that effective, and finally to identify serious gaps and shortfalls that need to be addressed. Our findings would then organized as a blueprint of sorts for the next presidential transition team.

One of the most important issues that people frequently reference is the lack of a comprehensive national strategy. I personally believe that the problem is not a lack of plans-we have far too many plans, in fact-but a failure to coordinate them on a strategic basis. Such a strategy should have two tracks. The first, in my view, should address near-term needs. The second, in turn, should address long term planning incorporating long term threats between five to ten years out. It is crucial these two efforts be symbiotic and run concurrently. Such an arrangement would lay the foundation for developing capital investment strategies for both our near and long term needs.

We must also consider the CBRN issue as it relates to prevention and preemption. Our priority should always be to prevent or disrupt a CBRN attack. This is not always possible, however, and we need to continue our efforts with respect to consequence management, as well as other ways to manage or mitigate risk.

Put simply, we need a complete set of golfs clubs in our national golf bag. Unfortunately, the Homeland Defense community is still looking at these issues in a piecemeal fashion. As Senator Roberts mentioned earlier, these issues are closely related and the lines between them blurred.

Yet regardless of whether these threats are national or international, they still require cohesive strategies.

A challenge of this magnitude also begs the question of whether we are properly organized to meet the CBRN challenge. Are existing policies, structures, and institutions adequate? CBRN terrorism is an inherently a cross-cutting issue. Yet despite this, the government is still structured along vertical lines. This issue requires coordination and cooperation among many people who have not yet sat around the same table. We need to be working towards a seamless integration of the national security, law enforcement, medical, and emergency response communities at the federal, state, and local level. This is quite a challenge.

Allow me make a few additional comments this morning regarding some of our findings. It is clear to me that our prevention efforts are insufficient, especially in terms of updating our deterrence strategies for both states and non-state actors. With respect to other states, I believe that we should unequivocally declare that the United States reserves the right to retaliate with nuclear weapons if our homeland, allies, or military forces are attacked with WMDs. As for non-state actors, we must make it clear to the leaders of terrorist organizations that they will be personally held accountable for their own actions and those of their subordinates. While our response may differ on a case-by-case basis, they should have no doubt that retribution is guaranteed. We should keep them on edge in much the same way they keep us on edge: that is, by not knowing when, where, or how we will respond.

We also need to reassess arms control as it related to non-proliferation and counterproliferation. There is no limit to the possible proliferation of CBRN arms and material, and there is no way they can be effectively monitored under the protocols enumerated in the Strategic Arms Reduction Talks (START) agreements. The United States should therefore take the lead in building international support for multinational monitoring of both states and the non-state actors that swim in their wake. Our working group is still exploring some of the options available to us in that regard.

The prevention and preemption of CBRN attacks is ultimately founded on good intelligence. Ideally, we would like to have a source within the decision loop of every terrorist organization, especially those that tend to germinate within very small cells. Such surveillance is nearly impossible, however. Our efforts must therefore focus on attacking these groups around the edges. Whether our objective is to string them up or string them along, we need to be able to identify and exploit whatever weaknesses they may have or develop.

A catastrophic CBRN attack on the homeland would strain the government beyond anything the United States has experienced in modern times. If such an event occurs, it will be extremely difficult for the President to explain the debates we are currently having within the beltway to the American people. Policy debates will not stand up in a crisis, and President's will be judged on the basis of their actions. We need to be willing to think beyond some of these debates.

With that in mind, there are two issues that we believe are significant. The first is FEMA. Let's be blunt: FEMA has become the cash machine for chasing hurricanes. They have dropped their black programs and their consequence management initiatives. Ideally, FEMA should be the lead federal agency for consequence management. They retain that nominal role under Presidential Decision Directories (PDD) 39 and 62 for consequence management. I think it is ludicrous to separate the agency responsible for consequence management from those agencies that are currently conducting preparedness exercises. This is exactly what we have done, however. Moreover, state and local authorities already know FEMA, largely through disaster management. In short, we need to think about how to get this agency up to the task. This should be considered along with additional efforts to maintain and sustain the Pentagon's civilian support capabilities.

Another important issue is the need to integrated authority and accountability with clear budget control. Whether it is an assistant to the president or and assistant to the vice president, there is a need for someone to have clear budget authority and oversight in the Homeland Defense area.

That said, we must always remember that in a no-warning catastrophic event the state and local responders will ultimately be at the tip of the spear. They are the ones who will decide weather a battle is won or lost. Despite budget limits, local responders must be able to transition from dealing to normal events, such as heart attacks and traffic accidents, to extraordinary events. Hence, one cannot overestimate the value of regular exercises and training. Training allows us to make the big mistakes in practice sessions.

Thanks to Dick Clark and others, I now have a poster the size of my office wall detailing the exercises undertaken by the federal government during the last eighteen months. Unfortunately, what may start in cities like Portsmouth, New Hampshire often stays in cities like Portsmouth, New Hampshire. What is learned at an exercise in Kansas often stays in Kansas. We need to synthesize new information and learn lessons from various exercises. That is why we propose establishing a federal clearing house for lessons learned in these exercises and work toward common best practices.

Let me finish my presentation by stressing the important of mobilizing and reinvigorating the public health and biomedical communities against bioterrorism and infectious disease. As Senator Roberts mentioned in his opening remarks, our preparedness for biological attacks is primarily a public health and medical matter. Yet to date, these communities remain largely in disarray. Only now are they slowly being integrated into the overall national security architecture. The fact is that there are many secondary and tertiary public health benefits that they public health community can offer the bioterror community, and vice versa.

There are two things we ought to be doing along the public health front. First is the need to recognize and redress the personnel retention problem though government personnel policies, pay scales, bonuses, and the like. The National Institutes of Health has had significant success in this respect. Unfortunately, that success is not universal in the federal government. At USAMERID, for example, loosing one person is often extremely disruptive. There is no private sector equivalent for their work, and no market for their vaccine research. Second, we need to appropriate emergency supplemental funding for CBRN response activities. During the NATO 50th anniversary Summit the Secret Service and several other agencies spend considerable sums on these security issues, sums they are not going to get back.

DR. JOSEPH COLLINS: Thank you Frank. It is now time for questions. Who would like to be first?

AMBASSADOR L. PAUL BREMER: I have a question regarding your organization proposal. It seems to me that any person or organization responsible for homeland defense needs two things: political accountability and budget authority. You achieve the first of these by assigning these tasks to the Vice President. I am unclear, however, about the Vice President's budget role under your proposal. Does the Vice President have the authority to overrule and certify like the Drug Czar? Who will run this proposed Emergency Planning Staff? Will that individual be confirmed by the U.S. Senate?

DR. JOSEPH COLLINS: In terms of the budget issue, there will likely be many federal departments that have budget line items dedicated to Homeland Defense. We have not proposed consolidating those resources. Rather, we saw the Vice President as someone who would have the authority, granted by the President, to oversee these budgets and to coordinate directly with the other relevant cabinet officers. Indeed, the Vice President would have more leverage given his position than would a mere cabinet officer.

As for the head of the Emergency Planning Staff, we currently envisage someone who would be the Vice President's chief of staff or primary advisor for this particular issue. It would preferably be someone with responsibilities not unlike those Dick Clark has today. The head of FEMA would not hold that particular portfolio.

AMBASSADOR BREMER: The proposal is an interesting one, but there are several areas where I believe it calls short. I think you need to think carefully about the role of the individual who has day-to-day operational control over this proposal staff. Confirmation by the Senate is essential in assuring that he or she has political accountability with Congress. That individual cannot merely be a staff person. As for budget control, you ought to look at the concept of built-in certification, a system used by the Drug Czar.

DR. JOHN HAMRE: I understand exactly what you are saying. This is one of those terrible dilemmas regarding how best to organize the government. The problem that Barry McCaffery has, however, is that he must sit down with the Secretary of Defense every year and plead to try to hold the line. That certification mechanism is not nearly as strong as people think it is. The real dilemma seems to be the problems caused by trying to consolidate budgets and the effect that has on behavior in the rest of the government.

DR. JOSEPH COLLINS: We would hope the Vice President would have more leverage in sorting out those issues. Again, this is a tough proposition.

STEPHEN HADLEY: Everyone says that the United States government will not be appropriately serious about these issues until there is some sort of accident or catastrophe. If you take that as true, then one of the best questions you can ask is whom you are going to fire. The problem with the Vice President is that you cannot fire him. You must determine who in the system has the kind of political accountability-the person whose head is going to roll.

DR. JOSEPH COLLINS: You may have a better view of this, Steven, given your background as a lawyer. I have been told that it is a non-starter to have anyone to suggest that anyone working within the Office of the President be confirmed by the U.S. Senate.

STEPHEN HADLEY: There are already a dozen or so people within the Office of the President that are confirmed by Congress, including the Director and Deputy Directors of the Office of Budget and Management, as well as the Drug Czar.

DR. JOSEPH COLLINS: Would that help or hinder your work from your standpoint as the national coordinator, Dick?

DICK CLARKE: It would mean that I would spend a lot more time up here on the Hill. (laughter)

SENATOR PAT ROBERTS: It became obvious to me that there were some difficulties here when we tried to put flags on some of the appropriations measures. This issue is very important, because it is very difficult for the thirteen appropriations subcommittee chairs and ranking members to find out who is in charge of the nation's Homeland Defense programs. That is a major undertaking. In the Defense Appropriations Bill, for example, we finally decided to give certain authorities to the Secretary of Defense rather than the Drug Czar. It turns out that the Secretary of Defense is the one person at the DOD charged with fighting terrorism who can come before the various Congressional Committees and Subcommittees and testify on the whole range of programs.

Organization is crucial, and we are not yet up to the task. With all due respect to the Congress and the Government Accounting Office (GAO), even the administration's relatively poor command of these budgets and programs is far better than our own.

FRANK CILLUFFO: We studied how to streamline and organize Homeland Defense appropriations at the committee and subcommittee level, and we recommended that there be a single staff member dedicated to these matters--someone who would look across all of these issues and develop a more comprehensive and integrated organizational plan. While we considered creating a special committee to address these matters, we ultimately determined that such an endeavor would ultimately create more unnecessary bureaucracy.

The more fundamental question, of course, is how to organize Congress. Indeed, if you want to streamline operations and establish clear authority in the Executive Branch, you must also do the same here in the Legislature. This is crucial for oversight purposes. Senator Roberts, what in your view would be the repercussions of such reforms here on the Hill, especially with regard to the committees and all their purse strings?

SENATOR PAT ROBERTS: It is a considerable dilemma. The fact is that many of us in the Senate are not fully aware of our colleagues' activities and their committees' jurisdictions. Those difficulties exist even within the majority.

DR. JOSEPH COLLINS: We have questions from Tony Cordesman, Phil Odeen, and Fred Iklé.

DR. TONY CORDESMAN: I would like to discuss a point that John Hamre made earlier. Frankly, a budget review is very easy to propose and very difficult to accomplish. Of the many billions of dollars dedicated to Homeland Defense, almost all of the funds go toward protection. What's more, those funds are allocated in line items in very small amounts, all of which affect federal spending in areas where a department or agency's primary role is frequently something else altogether. These line-item programs would be largely irrelevant in any broader crisis response given the funds that would need to be redirected from other federal spending in order to do the job.

Understanding the budget is further complicated by the fact that we have three program groupings. Indeed, neither the DOD nor the OMB reports on the subject coherently represent the various components of the Homeland Defense budget. For many of the most critical initiatives, there is no clear endgame, no clear cost estimates, no net technical assessments and no separate analysis of what it would be necessary for an adversary to overcome it. Many of these programs assume that no one will respond to new defensive or deterrent capabilities during the five to ten years following their development and deployment.

Frank's point is a good one. The fact is that budget authority in the classic sense will not give you a meaningful or effective program. If no one has conducted a net technical assessment regarding last month's technology, there is no way future changes in budget authority will accomplish anything. You must fundamentally reassess what you are asking various departments and agencies to accomplish.

PHILLIP ODEEN: I think your idea regarding the Vice President's role is an interesting one. Yet despite all of the discussion surrounding the various agencies and departments in the Homeland Defense architecture, the fact remains that the DOD has most of the necessary structures and capabilities.

DR. JOSEPH COLLINS: There are a whole series of organizational issues to address, and we will certainly have a great deal to say about the DOD's role. Their organization and decision-making is fairly advanced, and much of what happens in the Joint Forces Command and the Joint Task Force (civil support) will need more support in the long run. There are some issues that have not been resolved however. One is the existence of two separate chains of command within the Department itself. The first is for normal events, be they a flood, fire, or other natural or civil disaster. The second is for terrorist and WMD attacks. This fault line is not necessary. I believe

that we need to have one chain of command for consequence management in both civil emergencies and attacks on the homeland.

PHILLIP ODEEN: The second comment I have concerns the bioterrorism issue and widespread concerns regarding the readiness of our healthcare system. As health care providers move forward with the process of economic rationalization, excess patient capacity and catastrophic emergency response capabilities are being progressively reduced. This is an issue that needs to be addressed.

DR. JOSEPH COLLINS: That issue is central in our CBRN research. Our greatest concern is that modern economic pressures encourage hospitals to operate close to the margin, to avoid stockpiling, to practice just-in-time logistics, and to avoid purchasing or maintaining equipment that is not being used on a regular basis. A major trauma center in the Washington, DC area can currently be overwhelmed by a total of six people requiring ventilator support entering the emergency in a short period of time. When you start looking at these issues, it is clear that the medical community and the medical infrastructure is the weakest link in the chain. The scary part is that economic forces are telling those in this community—including the 30 percent of facilities that are not for making a profit—to operate closer and closer to the margin rather than building excess capacity for emergency situations.

PHILLIP ODEEN: Have you studied the question of whether states could establish requirements for ventilators, vaccines, and other catastrophic emergency preparedness measures in the hospital certification process? That is one way government can have some influence in this area.

FRANK CILLUFFO: We actually have a meeting with the Assistant Secretary of Public Health and several members of the medical community to discuss that question and many others tomorrow.

PHILLIP ODEEN: They will not like what you have to say. DR.

JOSEPH COLLINS: I agree. It is difficult to tell someone who is currently losing money that he or she needs to buy six ventilators that will be kept in storage.

DR. FRED IKLÉ: We have been talking a lot about consequence management this morning, rather than addressing the broader Homeland Defense issue. Certainly both issues are closely intertwined at an organizational level. We have, in effect, a two-tier threat. The first is terrorism, and the organizational structure to address that threat is emerging. The second tier is missile defense. No one here this morning has touched on this issue, despite the fact that it is implicitly related to the concerns that Phil Odeen raised.

We need to shift the focus of our thinking and our efforts from consequence management to the question of defense, broadly defined. A lot more can be done in this regard, and in addition to missile defense. Monitoring aircraft, trucks and ships carrying the instruments of asymmetric warfare is equally important.

DR. JOSEPH COLLINS: My view is somewhat different. I believe we need to use the assets that are already focused on the homeland's physical defense—institutions like the FBI and the Border Patrol. We intend to make several points about air defense and other related issues.

DR. DAN GOURÉ: Are you arguing that border interdiction ought to be a DOD issue?

DR. FRED IKLÉ: There are many ways to prevent asymmetric attacks in addition to missile defense. The presence of an armed vessel in the Port of New York or the transfer of chemical or

biological weapons across state lines are tasks for which only DOD is properly equipped and organized.

DR. DAN GOURÉ: So in effect, you would treat all of these domestically-based threats as a defense problem.

DR. FRED IKLÉ: If it is large. If not, then the FBI and other agencies should take the lead.

DR. TONY CORDESMAN: One of the things that struck me regarding the cyber warfare issue is that we tend to analyze what happens in relatively low-level attacks rather than addressing the capabilities other nations possess and the havoc they could wreck in open cyber warfare. The United States is in a poor position to assess both these concerns and our ability to respond to them. We have been told many times that given the fact that we currently have no offensive or retaliatory capabilities, our focus should be on defense. That bothers me. Has anyone ever simulated what an outside, state-driven cyber attack on the United States would actually look like—be it an isolated offensive or one conducted in conjunction with other non-cyber offensives?

FRANK CILLUFFO: One of the problems with cyber terrorism and cyber warfare is the attacker's anonymity. You are not always going to determine who is responsible for an attack. The same tools and techniques can be and are exploited by a broad range of potential foreign and domestic adversaries. Should we assess such threats in terms of the consequences or the actors?

DR. TONY CORDESMAN: Waiting for a real-world political crisis is an extremely dangerous way of approaching the problem, even if we are not expecting war with a known power.

DR. JOSEPH COLLINS: There is no end to the need for simulating such attacks and then developing and exercising our response to them. Even worse than the glaring lack of these simulations, however, is our inability to draw on our existing IT resources in a comprehensive way. We should not lose track of all that has been accomplished, however. This was an empty glass five years ago. Now that glass is half full. We must build on that work.

STEPHEN HADLEY: It is difficult to discuss many of these issues, and we often sanitize our concerns about war with language about deterrence. I believe we need to redefine what we mean by deterrence, with respect to both missile defense and many other issues. We are currently in a box where many believe it is easier to deter than to prevent hostile action. To accept that logic, you must have complete effectiveness. That model becomes a real barrier to understanding the broader problem. We need to think of defense as an element of deterrence and a means of strengthening deterrence. In that context, a missile defense or other defensive system need not be perfect in order to make a substantive contribution to our overall deterrence posture.

DR. JOSEPH COLLINS: We have been talking among ourselves about the importance of consequence management exercises and the deterrent value of openly publicizing whatever positive developments may result. The more potential terrorists believe we are able to deter or defend against certain attacks, the less likely they are to employ those potentially catastrophic means. We must be careful not to confuse the propaganda and the facts, however.

DR. DAN GOURÉ: I do not believe we have fully considered the offensive side of these equations. Regardless of whether an attack is from a terrorist, a state actor, or some combination of the two, we need the ability to strike back. That part of the equation has yet to receive honest consideration. If we are restricted only to consequence management, then we will lose. It may be that we need to reassess the question of preemption, even at the nuclear level. That may ultimately be a more rational response to many of these threats.

FRANK CILLUFFO: There is a need to personalize deterrence and tailor the means of retaliation. The question is how best to send the appropriate message. This is really a matter of compelling the right kind of behavior.

DR. JOSEPH COLLINS: Major General Ron Dardis of the Iowa National Guard is here today on behalf of the Governor of Iowa. Do you have any thoughts on these issues from the state level, General?

MAJOR GENERAL RON DARDIS: I would be very interested in hearing your thoughts on the integration of military with the first responder communities at the state and local level. We have our training and our capabilities on the military side. What about the civilian side? How do we ensure effective coordination and cooperation?

DR. JOSEPH COLLINS: It is still a tremendous problem. Back in 1996 the GAO issues a report saying that we have trained 134,000 emergency responders in integrated response. That may seem like a lot, but it is not. We estimate that the total number of emergency response personnel is somewhere around nine million. Even if that number is somewhat less-say around six and a half million-we have only reached about five percent of the first responder community in the last five or so years.

I recently visited an installation in Anniston, Alabama where the entire program was predicated on training the trainers. The program administrators estimate that nearly 30 percent of those completing the program actually conduct training exercises in their communities following graduation. We need to do more, and we have asked the Army what contributions they may be able to make with respect to expanding really sophisticated first-responder training in a live agent environment.

PHILLIP ODEEN: I know we have considered, and in some places started, a reallocation of National Guard's mission in combating threats of this nature.

DR. JOSEPH COLLINS: That is a difficult issue. The National Guard is a so-called "bellybutton" on any number of issues, including overseas warfare and peacekeeping operations.

FRANK CILLUFFO: There is a belief among some members of the National Guard that one of the primary reasons the Guard has been pushed into this domestic consequence management and mitigation missions was to exclude them from Active overseas operations. Does that belief still pervade the Guard's leadership?

GENERAL RON DARDIS: I would say that we are looking to the National Guard for new missions. We are looking at technology and methodologies that would allow us to collaborate with the Department of Defense at any level. This sort of network is not found anywhere else in the world. I would argue that the Guard is looking for new missions and is meeting the challenges they present.

DR. JOHN HAMRE: Iowa is a real case study for the development of new training and response capabilities at the state level.

DR. JOSEPH COLLINS: Thank you all for coming today. This session has been very helpful. I know that there are at least three or four important proposals and suggestions regarding our plan to better use of the Vice President in the Homeland Defense architecture that will help us refine our approach. We will continue to discuss these issues with you throughout the remainder of this year. Our next meeting will be this coming February.

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

"Defending America: Redefining the Concept of Homeland Defense"

Third Senior Advisory Group Meeting

September 12th, 2000

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

U.S. Capitol, Room HC-5

Participants

The Senior Advisory Group (SAG)

L. Paul Bremer

Managing Director

Kissinger Associates, Inc.

Richard Clarke*

Special Assistant to the President

National Security Council

Major General Ron Dardis Adjutant General Iowa National Guard (for Governor Thomas J. Vilsack)

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

Fred C. Iklé
Distinguished Scholar
CSIS

Bill Natter
Professional Staff Member
House Armed Services Committee (for Congressman Ike Skelton)

Philip A. Odeen
Executive Vice President of Washington Operations
TRW

The Honorable Pat Roberts
United States Senate

Bill Sutey
Legislative Assistant for
National Security Affairs

Dov S. Zakheim
CEO
System Planning Corporation International
Office of Senator Charles Robb (for Senator Robb)

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

Other Participants

Todd Anderson
International Security Program CSIS

Gabrielle Bowdoin
Research Associate
International Security Program
CSIS

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

Sharon Cardash
Research Associate Transnational Threats Initiative
CSIS

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

Daniel Gouré
Deputy Director, International Security Program
CSIS

Conrad Heede
Research Assistant

Larry Heftman
International Security Program
CSIS

Michael Horowitz
International Security Program
CSIS

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

Jeffrey Leary
CSIS

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

Andrew Li
Research Assistant
Burke Chair
CSIS

Alan McCurry
Military Legislative Assistant

Linnea P. Raine
Visiting Fellow Transnational Threats Initiative
CSIS

Daniel Rankin
Special Assistant to Harold Brown
CSIS

Susan B. Reingold
Visiting Fellow International Security Policy
CSIS

Colonel Joseph Rozek
USA Assistant to the Secretary of Defense for Civil Support

M. Jon Vondracek
Vice President for External Relations
CSIS