Testimony of

Dr. Philip Anderson
Senior Fellow and Director, Homeland Security Initiative

Center for Strategic and International Studies

Before the

Senate Governmental Affairs Committee

April 11, 2002

I. Introduction.

Mr. Chairman, my name is Phil Anderson, I am a senior fellow at the Center for Strategic and International Studies. I am grateful for the opportunity to testify before the committee today. (CSIS) is a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS seeks to inform and shape selected policy decisions in government and the private sector to meet the increasingly complex and difficult global challenges that leaders will confront in the years ahead. CSIS achieves this mission in four ways: by generating analysis that is anticipatory and interdisciplinary; by convening policy makers and other influential parties to assess key issues; by building structures for policy action; and by developing leaders. CSIS does not take specific public policy positions. As such, all views, positions, and conclusions expressed in this testimony should be understood to be solely those of the witness.

CSIS has completed a number of homeland security projects both prior to - and since the tragic events of September 11. In January 2001, CSIS released a report on the results of an eighteen-month study, *Homeland Defense: A Strategic Approach*. In June 2001, CSIS co-directed *Dark Winter*, a high-level simulation of a smallpox attack originating in Oklahoma City. In the immediate aftermath of September 11, CSIS convened an internal task force on terrorism, the results of which were published in *To Prevail: An American Strategy for the Campaign against Terrorism*.

CSIS is currently working on two projects in the area of Critical Infrastructure Protection:

1. A comprehensive series of events to address the urgent critical infrastructure issues facing the United States in this uncertain domestic security environment that will establish the foundation for a report that will focus on what business and government can accomplish together to meet future threats – pulling together public-private partnerships – with particular focus on leveraging technological innovation.

2. A simulation exercise, patterned after the Dark Winter effort, to focus on the vulnerability of U.S. energy infrastructure. Rather than consequence management, this simulation exercise will focus on the less understood - and explored - scenarios in which policymakers must decide on whether and how to act in the case of a credible threat against critical energy infrastructure. The events of September 11 and additional intelligence on al Qaeda demonstrate the potential for an attack against nuclear power plants, petro-chemical facilities, oil refineries, and liquid natural gas operations. The simulation exercise will focus on a number of important questions: In the event of a credible threat of attack, what should the government do? Should it interrupt operations at the facility or facilities involved in the threat? What should it do in the case of a general threat of attack against facilities without information about specific targets? How should decisions be coordinated with the private sector? How should they be communicated to the public? CSIS believes that a detailed discussion of this “real world” energy infrastructure scenario and its effects will serve the nation’s national security interests and help prepare the country to respond to this order of threat on its critical infrastructure.

II. Overview.

In the seven months since the tragic events of September 11, there has been a great deal of momentum, both inside and outside of government - and it would seem that we are all developing a clearer understanding of the Homeland Security problem in all of its complexity - but in this new environment, solutions remain elusive - which should be expected at this point - as we are barely seven months into a much deeper examination of the issue which in many ways represents the most daunting challenge the United States has ever had to address.

I was asked to comment on Senator Lieberman’s proposal to create a Department of National Homeland Security and a White House Office to combat terrorism. In this new and very dangerous environment, it appears that the proposed

legislation, if enacted, would greatly simplify management processes and unify the efforts of the 46 federal agencies that, to varying degrees, have responsibility for Homeland Security. Effective communication and coordination among these disparate agencies will be extremely complicated and over the long term, may be far too much to expect. With responsibility spread across so many agencies, it is equally difficult to ensure that no duplication of effort exists between organizational visions - and with the additional requirement for the federal government to coordinate and communicate efforts with state and local governments and further, to develop the means to work with, and cooperate with the private sector, it is clear that some organizational reform must be initiated to ensure accountability and unity of effort.

The most important question to consider at this juncture is: When should the federal government initiate organizational reform in order to address the Homeland Security requirement? Some would argue that there is no time to waste and that well-informed decisions should be acted on immediately in this environment. There are two problems associated with the desire to act now. First, an ongoing crisis may not be the best time to initiate organizational reform. With nearly every aspect of the National Security apparatus focused on the war on terrorism, such broad reaching change at this point in time could be an unwelcome distraction. Second and more importantly, in the absence of a comprehensive National Homeland Security Strategy, there can be no clear understanding of the threat to be addressed or any real sense of priorities from which specific requirements will emerge. It would seem that to organize in the absence of a strategy would be putting the proverbial cart before the horse. The strategy should serve as the basis to initiate organizational reform and allocate resources rather than the other way around.

The President has given Governor Ridge the task of developing a comprehensive strategy for National Homeland Security. It is the most important task for the Office of Homeland Security and I am confident that this is exactly what the dedicated men and women there are attempting to do. Assuming they can produce the strategy, and once it is on the table, the debate can begin on implementation. This will certainly involve a discussion on the appropriate organization of government to address the problem. Among the many organizational issues the strategy will have to address, the following would seem most important:

1. Create a foundation for unifying the efforts of the federal government or at least establish the conditions for effective cooperation and coordination.

2. Point the way for those agencies of the federal government, with direct responsibility for Homeland Security, to effectively cooperate, coordinate and communicate with state and local governments.

3. Establish the conditions for every level of government to effectively cooperate with the private sector since they own and operate most of the critical infrastructure in the United States and as such, are ultimately responsible for securing it.

Developing a National Homeland Security strategy that points the way toward effectively addressing these issues is no small task, it is truly a daunting challenge – the likes of which have never been faced at any other point in our Nation's history. It is important to note that despite the criticism in the media and on Capitol Hill - that the Office of Homeland Security is understaffed and has no budget authority or power to make decisions – the public should understand that the Administration has really not been given enough time to fully address this new challenge. While time is of the essence, this new environment demands at least some patience to allow a comprehensive strategy to emerge.

III. <u>The Challenges</u>.

There are numerous challenges associated with securing the homeland. The following are a few that should be considered in the development of proposed legislation:

A National Strategy as the for basis organizing the federal government: There have been numerous commissions and studies conducted - the Hart-Rudman Commission, the Gilmore Commission, the Bremer Commission, and the Center for Strategic and International Studies Working Group on Homeland Defense - that addressed the lack of coordination among the 46 federal agencies that have specific responsibilities for Homeland Security. Also, there have been a number of proposals floating around both in the Administration and in Congress that call for consolidating some of the agencies responsible for securing the homeland. The Administration's proposal to consolidate Immigration and Naturalization Service, Customs and the Border Patrol in one agency and the National Homeland Security and Combating Terrorism Act of 2002 are just two examples. Governor Ridge's original proposal also included the Coast Guard and border-related parts of the Agriculture Department. In addition, many commissions and studies recommended that

Congress develop the means for reviewing the President's policy and budget for Homeland Security. The lines of responsibility are unclear in the Executive branch but they are just as unclear in the Legislative branch with the existing committee structure that further complicates coordination in the Executive branch.

Most importantly, in the absence of a National strategy that establishes clear priorities and defines requirements, the basis does not exist from which decisions can be made about how to organize and spend the taxpayers' money. Significant organizational reform cannot happen without all the strategic underpinnings – the strategy in all its interrelated parts - that will allow government to make decisions on how best to organize. However, at various points in the development of the strategy, when information exists to support decisions, certain efficiencies could be gained by acting immediately.

Consolidation at any time will not be easy but will be far more difficult in the absence of a National Strategy. In addition, the agencies that will merge must bridge big culture gaps in missions to unify around the Homeland Security mission. Most of the agencies of government that are focused on Homeland security have other missions that will have to be accounted for. The Customs Service is a good example because it is more a revenue-generating agency focused on goods and trade than a security agency. Last year the Customs Service collected in $23.5 billion in taxes, fees, and penalties, second only to the Internal Revenue Service in generating government income.

Governor Ridge has a daunting task but one thing is certain, once a comprehensive National Strategy emerges, government must move forward as soon as practicable to organize itself appropriately to ensure the effective implementation of the strategy.

A comprehensive threat assessment as the basis for the National Strategy: It would seem that the administration has, since September 11, taken a "vulnerabilities-based" approach to the problem. That is, in the absence of a strategy, they have attempted to identify the Nation's critical vulnerabilities and focus attention and resources accordingly. Unfortunately, at this juncture, this is exactly the condition the public should expect where everything appears to be a critical vulnerability. This situation will not resolve itself until the Nation has a comprehensive Homeland Security strategy.

At the heart of any effort to develop a strategy will be the requirement to address the likely threats. The strategy that emerges at the end of the development process will need to be first and foremost, *threat-specific.* However, defining likely threats in this new environment is problematic in that they will likely derive from multiple sources with different objectives and various means to do us harm. Defining the threat is risky but absolutely necessary to developing a coherent National Strategy to address the problem. It is hard to develop plans, organize and allocate resources to address the myriad vulnerabilities that exist without taking an informed position on potential threats.

While we remain extremely vulnerable in many areas, most do not represent critical vulnerabilities simply because they are not likely targets. How many people would argue, at this point, that commercial aviation is a critical vulnerability? On the other hand, private aviation with 500,000 private pilots and 200,000 private aircraft operating from approximately 18,000 airfields could represent a critical vulnerability. Some would argue that the nuclear power industry is critically vulnerable. I would submit that the nuclear power industry, the most regulated in the United States, is far less vulnerable than other aspects of energy infrastructure to include, liquid natural gas operations, refineries and petro-chemical operations. The key point is that, without an informed assessment of how those that would do us harm may act, the ability to organize and allocate resources effectively is extraordinarily difficult, if not impossible.

Public-private partnership to ensure critical infrastructure protection: Much of the Nation's strength rests on its *privately-owned* critical infrastructure. The private sector is more aware than ever that critical infrastructure presents terrorists with a variety of attractive targets that remain vulnerable - but it still possesses limited awareness on how to protect infrastructure at risk. Despite its lack of experience, the private sector remains ultimately responsible for securing the infrastructure it owns and operates. This responsibility is complicated by the requirement to generate profits for stockholders and to provide customers with affordable service. Although the protections put in place by the private sector are essential, they cannot address all of the challenges by themselves. The federal government rightfully should share the burden for critical infrastructure protection. The federal government's role in infrastructure protection is complex and presents a different set of challenges. While the government cannot always assume responsibility for critical infrastructure protection, it must find ways to incentivize the private sector.

Developing public-private partnership is complicated by the need to protect sensitive information and the lack of organized communication and coordination between the numerous agencies of the federal government with responsibility for Homeland Security. The National Homeland Security Strategy must be the vehicle for simplifying the communication and coordination problem within government and between government and the private sector. It is essential that the private sector should be included in its development and implementation.

Simulation exercises and training to ensure readiness: Although expensive and time consuming, the federal government should develop and encourage simulation exercises and training at every level in the decision making process - that provide for state and local government and private sector participation. The purpose of these exercises should be to identify and improve the readiness of government and the private sector to carry out potential tasks and coordinate an effective response to all incidents, especially those that involve unconventional attack and the use of Chemical, Biological, Radiological, or Nuclear (CBRN) weapons. The response, clean up, and recovery effort that would be required following a CBRN attack - that synchronize decisions at the federal, state, and local levels as well as in the private sector - must be fully thought through.

Simulation exercises and training should be designed to develop greater public awareness and acceptance of risks and to address long-term economic recovery considering the implications of unconventional attack scenarios. While we would all like to believe CBRN attacks are a remote possibility, the evidence points to the contrary. How real the possibility that a terrible event like this could happen remains to be seen but it is clear that adequate preparation in the form of simulation exercises and training and education for unconventional attack is essential.

IV. Conclusion

Mr. Chairman, developing a National strategy to address this complex problem, under any circumstance, represents a daunting challenge but in the current environment where there is not a minute to spare, the pressures are enormous. When the strategy emerges, the real debate can begin so that every aspect of government can move forward together in a unified and coordinated way to fully address what is surely the most complex problem the Nation has ever had to face. I would ask you to consider the four challenges outlined in Part III of this testimony earlier, which I will address again:

A comprehensive National Strategy should serve as the basis for organizing the federal government for Homeland Security. Consolidation at any time will not be easy but will be far more difficult in the absence of a National Strategy. In the absence of a National strategy that establishes clear priorities and defines requirements, the basis does not exist from which decisions can be made about how to organize and spend the taxpayers' money. Most of the agencies of government that are focused on Homeland security have other missions that will have to be accounted for.

A comprehensive threat assessment should serve as the basis for the National Strategy. Clearly defining likely threats in this new environment is problematic but absolutely necessary to developing a coherent National Strategy to address the problem. Without an informed assessment of how those that would do us harm may act, the ability to organize and allocate resources effectively is extraordinarily difficult, if not impossible.

The means to create public-private partnership should be developed to ensure adequate security of critical infrastructure. The private sector remains ultimately responsible for securing the infrastructure it owns and operates. This responsibility is complicated by the requirement to generate profits for stockholders and to provide customers with affordable service. The federal government should share the burden for critical infrastructure protection, and while the government cannot always assume responsibility for critical infrastructure protection, it must find ways to incentivize the private sector. The National Homeland Security Strategy should be the vehicle for simplifying the communication and coordination problem between government and the private sector. It is essential that the private sector should be included in its development and implementation.

Simulation exercises and training should be developed to ensure readiness: Although expensive and time consuming, the federal government should develop and encourage simulation exercises and training and education at every level in the decision making process - that provide for state and local government and private sector participation. The response, clean up, and recovery effort that would be required following a Chemical, Biological, Radiological, or Nuclear (CBRN) attack - that synchronize decisions at the federal, state, and local levels as well as in the private sector - must be fully thought through. Simulation exercises and training should be designed to develop greater public awareness and acceptance of risks and to address long-term economic recovery considering the implications of unconventional attack scenarios.

Mr. Chairman, the road ahead remains complex and fraught with challenges yet to be addressed. The Center for Strategic and International Studies is ready and willing to help. Organizing effectively to secure the American homeland is essential to our country's prosperity and to the prosperity of our allies. We appreciate the Committee's leadership on this issue, and we look forward to helping in any way we can.