



214 Massachusetts Avenue, NE • Washington DC 20002 • (202) 546-4400 • [heritage.org](http://heritage.org)

*CONGRESSIONAL TESTIMONY*

---

**Risk and Resiliency: Developing the  
Right Homeland Security Public  
Policies for the Post-Bush Era**

**Testimony before the  
Sub-Committee on Transportation Security  
and Infrastructure Protection,  
Committee on Homeland Security  
United States House of Representatives**

**June 24, 2008**

**James Jay Carafano, Ph.D.  
Assistant Director of the Kathryn and Shelby Cullom  
Davis Institute for International Studies and a Senior  
Research Fellow for the Douglas and Sarah Allison  
Center for Foreign Policy Studies  
The Heritage Foundation**

My name is James Jay Carafano. I am the Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and a Senior Research Fellow for the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation. The views I express in this testimony are my own, and should not be construed as representing any official position of The Heritage Foundation.

Thank you for the opportunity to appear before the committee today to discuss the subject of this hearing “Ensuring our Nation is secure by developing a risk management framework for Homeland Security, How are they measuring risk? Are the risk management principles being followed uniformly?”

My testimony today will focus on the point that risk management is interwoven with the concept of resiliency. The current paradigm of “protecting” infrastructure is unrealistic. We should shift our focus to that of resiliency. Resiliency is the capacity to maintain continuity of activities even in the face of threats, disaster, and adversity. The concept recognizes that we cannot deter all threats or prevent all natural catastrophes. Effective resiliency strategy should:

- **Focus on more than just physical infrastructure** – resiliency works with the goal of resilient communities and reflects the geography, culture, economy, politics and other societal factors of the United States.
- **Recognize initiatives must be national in character and international in scope.** Recognizes that America is part of the global marketplace with a global industrial base.
- **Remain proactive.** It is a bad idea to wait until catastrophe strikes to discover our resilience, in terms of both humanitarian concerns and government legitimacy.
- **Manage public expectations-** Out-of-scale expectations greatly undermine the legitimacy of a national response effort. We must inform the public about what it should reasonably expect in the face of disaster or disruptions. Unreasonable expectations are fueled by both media and political posturing.
- **Define expectations of public-private partnerships.** Despite the focus on homeland security since 9/11, five years after the event the appropriate public and private rolls in dealing with transnational terrorist threats are still poorly understood.
- **Pay greater attention to the development of public and private infrastructure.** Developing more robust national infrastructure that both enhance the competitiveness and capacity of the US to withstand catastrophic threats should be a priority.

**Resiliency and Risk.** Risk assessments and risk reduction are at the heart of a sound resiliency strategy. Although there are a number of risk assessment methodologies, they all consist of common components.

- *Threat Assessment*- Examines what our adversary can accomplish and with what degree of lethality or effect.
- *Criticality Assessment*. Evaluates the effect that will be achieved if the adversary accomplishes his goals. This examines both physical consequences, social and economic disruption and psychological effects. Not all consequences can be prevented. So in order to assist in prioritization, there is a process designed to identify the criticality of various assets: What is the asset's function or mission and how significant is it?
- *Vulnerability Assessment*. Looks at our vulnerabilities and how they can be mitigated including weaknesses in structures (both physical and cyber) and other systems/processes that could be exploited by a terrorist. It then asks what options there are to reduce the vulnerabilities identified or, if feasible, eliminate them.

Since 9/11, however, the nature of shared public-private responsibility for risk assessment and risk reduction has been poorly understood. Establishing a common appreciation of rolls and responsibilities must be a priority.

- Assessing and reducing transnational terrorist threats is fundamentally a government responsibility, an inherent obligation derived from the preamble of the Constitution that obligates government to "provide for the common defense." Threat appreciation and effective counter-terrorism programs that identify, quantify, and reduce threats is not only primarily government's responsibility, it is arguably the most essential component of risk management. Taking the offensive against terrorist threats is both the most effective and cost-effective means to respond to transnational terrorism.
- Criticality is an activity that must be conducted jointly by the public and private sectors. They equally share responsibility for determining what is most vital to protect the public good. There is no practical alternative to this shared obligation. Most national infrastructure is private hands. The private sector understands best how systems function and impact the economy. On the other hand, only the national government can offer the national "perspective" of prioritizing needs and obligations in times of national emergency. Thus, criticality can only be determined by sharing information and joint assessments made in trust and confidence between the public and private sectors.
- Assessing vulnerability, determining the best risk mitigation means, managing and providing the resources to reduce vulnerability are largely the responsibility of the entity that owns and operates infrastructure. Most often the consumers and users of the infrastructure and the services they provide bear the fiscal responsibility for implementing measures to reduce vulnerability. These measures should be "reasonable." Vulnerability reduction is an "economy of force" measure, an additional and supplementary line of defense designed to supplement not supplant addressing threats and criticality. Over-emphasis on vulnerability

reductions threatens the competitiveness of private sector activity, which in turn could represent a far greater threat to the resiliency of the American economy than any terrorist threat.

Understanding this fundamental division of labor between the public and private sector is fundamental to developing sound public policies.

In order to achieve the goal of “resiliency” as well as to ensure effective risk management, Congress should focus on four initiatives:

- 1. Promote public-private models for risk management by developing doctrine defining reasonable roles for government and industry.**
- 2. Encourage bilateral cooperation addressing liability issues.**
- 3. Develop national and international forums for collaboration on resiliency issues.**
- 4. Promote the development of resilient 21<sup>st</sup> century public infrastructure.**

**1. Public-private models for risk management.** Public-private models for risk management are essential to the concept of resiliency. A model public-private regime would: (1) define reasonable roles for both government and industry through clear performance measures, (2) create transparency and the means to measure performance, and (3) provide legal protections to encourage information sharing and initiative.

Both government and industry must be given reasonable roles in order to ensure the effectiveness of these models. Understanding, communicating, and reducing threats is primarily a national responsibility, fundamentally a responsibility of government to ensure public safety and provide for the common defense. It is not the job of the private sector to defeat terrorists. It is the responsibility of the federal government to prevent terrorist acts through intelligence gathering, early warning, and domestic counterterrorism.

**National Security and Resiliency.** In terms of what is reasonable for the government, the role of national security instruments should be treated with caution. National security is not about trying to child-proof a country against every potential misfortune. It is the task of protecting people from their mortal enemies—that means other people. These enemies may be from states, trans-states or no states. They may be abroad or homegrown. What they have in common is that they are humans—and that they threaten the nation by preparing to attack its people for a political purpose.

We should be careful not to dilute the definition of national security to include a plethora of threats or use the proliferation of threats to scope a national resiliency strategy. The Government has many resources to deal with all kinds of problems. Resources, however, are not infinite. National security instruments should be reserved for the critical task of

battling those people who plot how to kill citizens, undermine the society and destroy our individual freedoms.

A second reason not to label every “danger du jour” as a national security threat concerns protecting the civil society. In times of peril, the nation should rely on the government to provide the common defense— providing the leadership and resolve needed to deal with threats to the nation. That’s why, for example, in the United States the president is vested with the authority to conduct foreign policy and act as commander-in-chief. The U.S. Constitution envisioned an executive who could wield significant power to act decisively in time of war or crisis. That said, the president’s national security powers should be reserved only for serious, imminent dangers from America’s enemies. Elevating other issues like global warming, pandemics or energy supplies, to the level of national security, only encourages government to bring the extraordinary powers of the executive branch to bear on the problem. For the most part, the parts of government involved in national security should stick to hunting terrorists, thwarting rogue states, and dealing with the other serious enemies who spend their days and nights plotting against the state. In most cases a strategy of resiliency should rely primarily on other instruments.

**Criticality as a Shared Activity.** Criticality, on the other hand, has to be a shared activity. In many cases the private sector owns or is responsible for managing both private and public infrastructure that provide the vital goods and services for the society. Meanwhile, only the national government has the overall perspective to determine national needs and priorities in the face disasters and catastrophic threats. Thus, they must work together to determine what is truly critical to keep the heart beat of the nation beating in the face of adversity.

Not all infrastructure should be deemed critical. Indeed, the national designations of “critical” infrastructure and key assets have been detrimental to the effort to prioritize national efforts. The “failure is not an option” mentality with regards to protecting infrastructure has led to an over-zealous approach to “critical” infrastructure. The designation has become increasingly pointless driven by politics and stakeholder interests rather than rationale assessments.<sup>1</sup> If everything is critical, nothing is critical.

**Vulnerability as a Private Sector Function.** Vulnerability should be largely the responsibility of the entity that owns, manages, and uses the infrastructure. It is largely the private sector’s duty to address vulnerability and to take reasonable precautions, in much the same way as society expects it to take reasonable safety and environmental measures.

Resiliency and its role in protecting society actually transcend homeland security and other national security concerns. Resiliency is about building strong, cohesive societies in that can prevail in the face of many challenges whether the malicious acts of terrorists or the heartless whims of Mother Nature.

---

<sup>1</sup> See, for example, the debate over container security in “Container Security at U.S. Ports: The Heritage Foundation’s Research,” *WebMemo #1260*, November 27, 2006, at <http://www.heritage.org/Research/HomelandSecurity/wm1260.cfm>.

Indeed, rather than national security instruments, the most common tool to be used in building resiliency is establishing an appropriate legal regime that will allow the private sector and the market place to adapt and innovate, to provide a robust, redundant capacity to provide goods and services everyday—and especially in times of crisis.

Armed with these assessments and a common sense division of roles and responsibilities, public-private partnerships can set about instituting practical measures that will reduce risk and enhance resiliency.

**2. Encourage bilateral cooperation addressing liability issues.** Addressing concerns of liability may be the most vital contribution government can make to implement a strategy of resiliency. The recent bitter debate in the United States between Congress and the administration over extending immunity against civil suits to telecommunications companies that cooperated with a classified government surveillance program highlights one of the knotty challenges in promoting public-private cooperation in combating terrorism.<sup>2</sup> Congress can promote private sector participation and alleviate liability concerns by:

- **Providing ‘safe harbors’ for sharing critical information**
- **Promoting cooperative joint action for public-private partnerships**
- **Collaborating with other nations, such as the Technical Cooperation Program (TTCP), an inter-national organization that collaborates in defense scientific and technical information exchange and shared research activities. Promoting liability protection regimes could be the centerpiece of a facilitating global bilateral participation in promoting resiliency strategies.**<sup>3</sup>

**The Safety Act as a Model for Liability Concerns.** A great example of the ability of government to handle these concerns over liability decisively and with good effect was addressed in the Support Antiterrorism by Fostering Effective Technologies (SAFETY) Act. This Act lowered the liability risks of manufacturers that provide products and services for combating terrorism. Passed in 2002, the Act protects the incentive to produce products designated as “Qualified Anti-terrorism Technologies” (QATTs) by the Secretary for Homeland Security. The Department of Homeland Security (DHS) has made a concerted effort to implement the program and a number of companies have availed themselves of the opportunity to obtain SAFETY Act certification.

By addressing liability concerns, Congress intended the SAFETY Act to serve as a critical tool for promoting the creation, proliferation and use of technologies to fight

---

<sup>2</sup> See, James Jay Carafano, Robert Alt, and Andrew Grossman, “Congress Must Stop Playing Politics with FISA and National Security,” *Web Memo #1791*, January 31, 2006, at <http://www.heritage.org/Research/LegalIssues/wm1791.cfm>.

<sup>3</sup> For specific recommendations, see James Jay Carafano, Jonah J. Czerwinski, and Richard Weitz, “Homeland Security Technology, Global Partnerships, and Winning the Long War,” Heritage Foundation *Backgrounder* No. 1977, October 5, 2006, at [www.heritage.org/Research/HomelandSecurity/bg1977.cfm](http://www.heritage.org/Research/HomelandSecurity/bg1977.cfm).

terrorism.<sup>4</sup> The act provides risk and litigation management protections for businesses that produce QATTs and other providers in the supply and distribution chain. The act included a limitation on liability with regards to third parties claims for losses resulting from an act of terrorism where the technologies were deployed to help prevent or mitigate the danger of a terrorist attack. In turn, the promotion and deployment of new technologies help make the society more resilient in the face of terrorist threats.

**3. Develop national and international forums for collaboration on resiliency issues.** Both within the United States and with international partners, the United States should begin to establish regular forums to promote the resiliency concept, share best practices and facilitate joint action.

**State-Based Regional Response Network.** Within the United States, these forums could be structured around a regional homeland security structure that promotes voluntary cooperation among states, local communities, and the private sector. The Homeland Security Act of 2002 mandated that DHS set up a regional structure--though the department did follow through on this mandate. State-based regional programs would focus on ensuring that states are prepared to sustain themselves. Successful regional programs would focus not on federal structures in each region, but rather on regional emergency management programs and capabilities that are developed, coordinated, and managed by the states. Similar small-scale programs that use a regional model, such as the Emergency Management Assistance Compact (EMAC), have already proven successful. DHS regional offices should be required to strengthen state and local preparedness capabilities; facilitate regional cooperation among governments, the private sector, and non-governmental organizations; and plan and exercise with federal entities that support regional disaster response. Such offices would enable regions to access and integrate their capabilities quickly and improve preparedness and resiliency initiatives.<sup>5</sup>

Internationally, the United States can use both current international institutions and new multi-national and bilateral partnerships to create resiliency forums. For example, the NATO Industrial Advisory Group (NIAG) solicits industry advice on how to promote public-private and transnational cooperation in defense production. This group or other NATO forums might serve as opportunities to discuss resiliency issues.

**4. Resiliency's Building Blocks -- Promote the development of resilient 21<sup>st</sup> century public infrastructure.** In the end, public-private partnerships must produce the kind of infrastructure necessary to sustain 21<sup>st</sup> century societies against 21<sup>st</sup> century threats. Within the U.S. much of the national infrastructure is aging and not keeping up with the demands of a growing population. Additionally, for all of the focus on U.S. critical infrastructure, equally vital is the resiliency of the global economy.

---

<sup>4</sup> U.S. Department of Homeland Security, *Final Rule of the Implementation of the SAFETY Act*, Vol. 71, June 2006, at <http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/06-5223.htm> (March 2008).

<sup>5</sup> See, Jill Rhodes and James Jay Carafano, "State and Regional Responses to Disasters: Solving the 72-Hour Problem," *Backgrounder #1962* (August 21, 2006) <http://www.heritage.org/Research/HomelandSecurity/bg1962.cfm>.

What is required is more innovation and experimentation as a means of speeding the development of modern infrastructure. One option to consider is encouraging public-private partnerships (PPP) that invest in public infrastructure. The U.S. has utilized the PPP model for its public highways and other infrastructure projects. Creating opportunities for governments and private firms to work together on improving the infrastructure should be further explored.

Rather than relying heavily on subsidized public funding of infrastructure, investments should focus on “project-based” financing that shifts the risks and rewards to the private sector. Project-based financing focuses on obtaining stand-alone investment from private investors and could include multiple investors, each with a different level of investment, varying rate of return, and different timelines for realizing those returns. Such strategies not only shift risk to the private sector, but should also lead to improved decision-making about needed infrastructure investments.

**Resilience is the right strategy.** Resiliency is the right strategy for the United States and its allies in facing the dangers of the 21<sup>st</sup> century. Congress and the Administration can promote this approach both within American communities and across all free nations by means of the initiatives mentioned in my testimony. These initiatives offer a more reasonable and cost-effective means for ensuring the continuity of services and processes, but all for building a more resilient civil society, one prepared to face the future with confidence and surety.

\*\*\*\*\*

The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(C)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2007, it had nearly 330,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2007 income came from the following sources:

Individuals	46%
Foundations	22%
Corporations	3%
Investment Income	28%
Publication Sales and Other	0%

The top five corporate givers provided The Heritage Foundation with 1.8% of its 2007 income. The Heritage Foundation's books are audited annually by the national accounting firm of McGladrey & Pullen. A list of major donors is available from The Heritage Foundation upon request.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own, and do not reflect an institutional position for The Heritage Foundation or its board of trustees.