Summary of 2008 Homeland Security Symposium at the National Academies: Fostering Public-Private Partnerships

George H Baker, *James Madison University*
Cheryl J Elliott, *James Madison University*
Summary of the Proceedings of the 2008 Homeland Security Symposium
Fostering Public-Private Partnerships

by Dr. George H. Baker, Associate Director for Infrastructure Assurance, and Cheryl J. Elliott, Assistant Director for Marketing and External Relations, JMU IIIA

The theme of the third annual JMU IIIA Homeland Security Symposium, Fostering Public-Private Partnerships, was based on an important conclusion from our 2007 symposium, Cascading Infrastructure Failure: Avoidance and Response. Recent U.S. high-consequence events have clarified the importance of government collaboration with industry. The benefit of such collaboration was one of the most important lessons learned from Hurricane Katrina. The resources owned and controlled by American industry dwarf those available to local, state, and even federal government departments. Better agreements and incentives to bring the full capabilities of industry squarely into the national response agenda will be indispensable in effectively responding to large-scale catastrophes. At our 2007 symposium, General Russel Horne, who led the National Guard response to Katrina stated, “We need the partnering between local, state, and federal governments; but the biggest partner should be industry . . . because people in industry, if they understand the problems, can take them on as business opportunities.”

The 2008 event program was structured to illuminate exemplary public-private partnerships at the local, regional, and national levels and consider steps to develop and improve public-private partnerships for the future. The program included presentations by recognized experts from government and industry engaged in operating and securing critical infrastructures. Participants represented academic, federal/state/local government agencies, private sector companies, industry associations, and standards organizations.

Morning Keynote

Congressman Dutch Ruppersberger, Maryland 2nd District, serves on the Appropriations Committee; the Technical and Tactical Intelligence Subcommittee; the Terrorism, Human Intelligence, Analysis, and Counterintelligence Subcommittee; and the Oversight and Investigations Subcommittee.

Congressman Dutch Ruppersberger (MD-2) emphasized the importance of government-industry partnerships, but also stressed the importance of academia in solving homeland security problems. His district relies heavily on expertise from Johns Hopkins University, the University of Maryland, and Towson University. His talk focused on two technical areas in need of improved public-private partnerships: intelligence satellites and cyber security. In these areas, two domains come into play — real space and virtual space. With respect to intelligence satellites, the government owns the satellite hardware and defines the projects and parameters. Yet, most of the work associated with satellite development is done through the private sector. Cyber security is an area where the government has only limited control because the networks and enterprises are mostly privately owned and controlled. Both areas require strong partnerships between government, industry, and academia if our national security is to be ensured.

Speech Excerpt:

A major source of U.S. strength is our ability to control the skies. Our ability to control the skies is being challenged by other nations, notably Russia and China. To maintain our capabilities, we need to build the next generation of satellites quickly. Private sector involvement with its best practices and expertise is critical for success.

Development timeline and costs of satellites are increasing. After Sputnik, President Kennedy challenged the technical community to achieve a moon landing. NASA seized the initiative and achieved this objective in twelve years. At present, we have difficulty developing and deploying a satellite in twelve years. It is clear we need to put a higher premium on R&D in the U.S. Intelligence
Satellite showstoppers are worrisome given the challenges posed by Russia and China.

Many of the problems are results of the lack of communication between government and industry. Contractors are not asked the right questions in the Request for Information (RFI) process. Contractors are not clear on requirements. The government often rushes to get RFIs out against arbitrary deadlines. It is often assumed that uncertainties, specifications and unknown factors inherent in RFIs can be fixed by future renegotiation; however, we need to plan for unknowns up front.

Satellite procurement problems are easy to solve compared to cyber security. In the case of satellites, the government can specify performance requirements. Since the government does not control Internet, it is very difficult to secure, especially so, considering everything connected to it. Ninety-eight percent of Internet traffic runs on private networks. The Internet is "owned by everyone . . . controlled by no one."

A major objective with respect to cyber security is protecting the banking sector. Bank networks are continuously under attack. A major successful attack would result in an unprecedented bank run. Financial markets would panic. Even if the network were only down for a day there would be catastrophic consequence for our economy.

A network is only secure as its weakest point. Our national security networks are connected to the outside world. The ability to disrupt our networks has fundamentally altered the strategic landscape. Public-private partnerships are essential to secure every network in the U.S. because the government cannot decide how to organize and secure the Internet and then hire someone to do it. Every company with a server in its back room needs to be involved with this effort. Universities play a major role in growing our network security workforce.

**Panel 1 - Local Public-Private Partnership: Nassau County, New York's Security/Police Information Network**

**Panelists:** Assist. Chief Paul Tully, Nassau County Police Department; Moderator: Detective Sergeant William Lindley, SPIN Coordinator, Homeland Security and Counterterrorism Bureau, Nassau County Police Department; Ossama Farber, insurance industry professional; and Maria Doyle, Director of the Police Reserve Force for Nassau County.

The Security/Police Information Network (SPIN) is a dynamic, multi-dimensional crime prevention partnership including Nassau County Police Department, the public, and business. It connects federal, state, and local government agencies with transportation and other infrastructure services. It is essentially a virtual public-private partnership (VP3) that seeks to increase public safety through the sharing of important and timely information.

The network is organized into concentric rings. Federal/state/local law enforcement is in the center. Government is the second ring. Critical infrastructure service providers and individual businesses are the third, outer ring. Created by the Nassau County Police Department in 2004, SPIN utilizes e-mail coupled with live meetings to provide private sector partners with the information they need to protect themselves, their families, their communities, and their organizations. In addition, the VP3 has enabled the Police Department to leverage the private sector in order to prevent crime, arrest offenders, and otherwise maintain safer communities.

Taking an "all-crimes, all-threats, all-hazards" approach to information sharing, SPIN supports wide-ranging missions — from homeland security and business continuity to crime prevention and emergency preparedness. This broad approach is not only advantageous to private sector partners, but facilitates intergovernmental partnerships, as the need for information has brought about collaboration between the Police Department and the Office of Emergency Management, Department of Health, the Fire Commission, and the local public transportation agency. The network has grown exponentially from 175 security directors at its inception to more than 800 security directors from nearly every sector and critical infrastructure, 125 business and community leaders, 100 government employees, and over 300 members of federal, state, and local law enforcement.
PANEL 2 – Regional Public-Private Partnership: Mid-Atlantic States All Hazards Consortium (AHC)

Panelists: Honorable Robert Crouch, Assistant to the Governor for Commonwealth Preparedness; Moderator: John Contresible, Director of Engineering & Emergency Services, Maryland Department of Transportation; David Lindstrom, Chief Privacy Officer, Pennsylvania State University; and Michael Hughes, Northeast Program Development Manager, Northrop Grumman Corporation.

According to its website, “The All Hazards Consortium was built on the belief that state/federal government is ultimately responsible for the protection of the public. Based on this assumption, the AHC sees government as the ‘owner of the problem.’ The private sector owns most of the assets, technologies and solutions; the universities provide research and education to address the problem; and non-profit organizations provide access to information and people who are focused on a particular segment of the problem. By bringing together all stakeholder groups into regional Advisory Committees, Working Groups and ad hoc committees, and focusing on specific issues (with state government driving the need), a powerful environment for collaboration is created to solve tough problems that require resources from every sector.”

The AHC acts as a facilitator to bring the stakeholders together from nine Mid-Atlantic states to share information, collaborate in addressing possible solutions to regional homeland security challenges, identify funding sources, and develop regional initiatives that produce results.

The organizers have found that the best information sharing occurs using the workshop venue. The operating slogan is “be responsive to those who own the problem.” Based on the workshop deliberations, the AHC produces white papers to be shared with federal agencies and cognizant congressional staff. The white papers’ recommendations form the basis for multijurisdictional funding proposals. Workshop topics (and subsequent white papers) have included interoperability, catastrophic evacuation planning, fusion centers, and critical infrastructure protection. In July 2008, the AHC is sponsoring a GIS workshop at Towson.

The AHC incorporates the elements of people, process, and technology, paying particular attention to people and process. It is not possible to move to the implementation phase without having people working together across jurisdictions and across disciplines. The AHC is currently addressing more than 20 region-level homeland security and emergency management issues that the member states have identified.

The Role of Academia
The role of higher education in the AHC includes education, research, community outreach, and government service. Universities are often affordable; modest funding can reap major benefits due to the intellectual capital available. The AHC allows higher education to connect with the people owning the problems, figuring out who has the necessary resources, and how collaborations for solutions can be created.

The Role of the Private Sector
Within AHC workshops, private sector representatives are willing to share their issues, needs, and challenges, as well as information, assets, technologies, and solutions. Though not a direct pipeline for business development opportunities or contracts, the AHC provides a unique listening opportunity for private business to interact with end users. The AHC provides a level playing field for contractors. This interaction allows for more intelligent requests for proposals (RFPs) to be issued and for more in-depth cross-jurisdictional collaborations.

A critical lesson from this partnership is the importance of two bedrock principles: trust and focus on priority problems. Trust must be engendered across the disciplines and jurisdictions, or they will not stay engaged. As long as focus remains on the problem and trust is maintained amongst the parties, collaboration is possible. When either of those two tenets is violated, there will be problems.

PANEL 3 – National Public-Private Partnership: The National Security Telecommunications Advisory Committee Telecommunications/Electric Interdependency

Panelists: Dr. John S. Edwards, Nortel Designated Representative
to the NSTAC's Industry Executive Subcommittee, Moderator: Daniel C. Hurley, Jr., Director, Critical Infrastructure Protection, U.S. Department of Commerce, National Telecommunications and Information Administration, and Chair of the Communications Dependency on Electric Power Working Group (CDEP WG); and Lawrence Hale, Acting Director, National Communications System (NCS).

The President's National Security Telecommunications Advisory Committee (NSTAC) has a 25-year history of government-industry partnership with several important contributions to assure the security of the Nation's telecommunications service. Recently, NSTAC sent to the President a two-part report on the interdependency between telecommunications and electric power services. The first part, "People and Processes," covered access control measures and cooperation in the aftermath of natural and man-made disasters. The second part, discussed issues related to what the Committee described as "Long Term Outages" and addressed measures to mitigate effects, recover operations, and methods to reduce the likelihood in advance.

Both reports were based on collaboration between the telecommunications and electric power industries and the governments of Canada and the United States. Although NSTAC sponsored and led the effort, a unique collection of subject-matter experts from the telecommunications and electric power industries, and government from both countries met collegially over a two-year period. The reports were submitted to President Bush and as a result, the government established a Communications Dependency on Electric Power Working Group (CDEP WG).

Mr. Dan Hurley chairs the CDEP WG. Its mission is to research and report on issues relating to long term outages. It is a difficult problem because the longest outage our nation has had only lasted about two weeks. The CDEP WG is looking at situational awareness tools and their usefulness in coordinating with other critical infrastructure sectors. It is also looking at new technologies for backup power, including fuel cells, wind power, photovoltaics, and recovery transformers. The WG should have an initial draft report on its findings by the end of summer 2008.

NSTAC industry subcommittees are ongoing and productive. The government supports NSTAC primarily by providing information; government representatives do not get involved in deliberations. Some examples of areas being addressed by NSTAC include:

- Emergency communications and interoperability – task force established
- Assessment of dependence on GPS and implications of loss or disruption – task force established
- Global infrastructure resiliency
- Examination of legislative and regulatory developments
- Examination and report on Estonia cyber attacks
- Network security

One significant example of a public-private partnership began in 2003, when Dr. Jack Edwards was asked by then-NSTAC Chair Duane Ackerman to head an interdependency task force. NSTAC had, in the past, addressed "dependency," but not interdependency." For instance, dependency studies had looked at the vulnerability of supervisory control and data acquisition (SCADA) systems. Mr. Ackerman asked two fundamental questions: (1) how do the telecommunications and electric power infrastructures rely on each other? and (2) how would they need to be rebuilt if they were both down for a period of time? The Interdependency Task Force first met in the spring preceding Hurricane Katrina. Katrina provided a useful case study for the group's after-action report.

This Task Force reached out beyond the telecommunications industry to include members of the electric power and other private industries and government organizations in the United States and Canada. In North America there is no distinction between Canada and the United States in electric power and telecommunications. However, there are big differences in viewpoints between the telecommunications and electric power industries concerning outages. The Task Force concluded that a very strong situational analysis tool is needed to work with fusion centers to develop a composite picture of large-scale outages.

NSTAC government-industry partnerships have demonstrated that there are major economic benefits of
public-private partnerships. Government interaction with industry is essential to improving the resilience of our critical networks.

Afternoon Keynote


As Assistant Secretary for the Private Sector Office of DHS, Martinez-Fonts described the 2002 law that created DHS, which also gave his office seven tasks to achieve. Subsequent laws over the last six years have added four more tasks, bringing the total to 11 unique mandates.

Speech Excerpt:

First and foremost, we are to advocate clearly on strategic issues for the private sector. If you are in the private sector, I'm the guy you want to know in the Department. I don't have a budget. I don't buy things, and I'm not on the procurement side.

The second thing that we do is share information and best practices. I don't create the information. What we try to do is make sure that we can bring that information in at an unclassified level to share it with more people and businesses and to make it actionable. Do I need to put some guards on the back gate? Do I need to change the HVAC system? Do I need to stop a truck from coming into my facility? We do our best to get information out that is important to the private sector, especially information on best practices for areas such as pandemic influenza and telecommuting.

In the Private Sector Office, public-private partnerships are clearly the cornerstone of our mission, and both sides need to be present to solve homeland security problems. There is a need for a champion ... someone who will sometimes put his neck on the line to make sure this thing gets done.

The example I will relate occurred at a border port. On one side is the port of Nogales, Arizona. On the other side is the port of Nogales, Sonora. It is one of the busiest ports on the southern border. The joke in Nogales was, as a member of [Customs-Trade Partnership Against Terrorism] C-TPAT, it takes you two hours to get across the border. As a non-member it takes you two hours and one minute. It was clear that we needed to build infrastructure to improve the throughput of the last stretch. The projected price was $10 million. The partnership did not happen automatically — it took a lot of work and pushing to get the stakeholders together to do it, but the end result was more lanes built, shorter time frame and the cost reduced to $3.2 million.

Another example is from Assistant Secretary [for Infrastructure Protection] Bob Stephan. I view the Critical Infrastructure Partnership Advisory Council or CIPAC as one of the all time greatest public-private partnerships. The CIPAC is really a process under which we have created now 18 self-organized critical infrastructure councils. It is like that old Saturday Night Live, "talk amongst yourselves" routine. Go over there, bankers, and talk amongst yourselves.

Go over there, energy people, and telecommunications people and so on and talk amongst yourselves. We then brought the government side together and said, if you want to talk among yourselves, you need to make sure that you include the private sector.

In order for the CIPAC to work, it was very important to address possible problems due to the Federal Advisory Committee Act or FACA. The Secretary used his authority to exempt the entire CIPAC group from FACA. It was not a case of the government trying to hide things. If discussions at CIPAC meetings were published in the Washington Post or the New York Times, so on we would talk. So we needed to have a legal structure that would exempt us from FACA and allow us to have the kind of relationship we needed among the private sector companies and not importantly the industry sector and the government. CIPAC created that protective space so that the CIPAC includes sector coordinating councils and government coordinating councils.

This partnership has been invaluable in enabling discussions among interdependent infrastructure communities, essential to protecting our critical assets. To me this is one of the greatest examples of a public-private partnership and I have been much impressed with the enthusiasm and buy-in that we have had from all of the sectors.

Being able to create public-private partnerships, I am convinced, is the way that we are going to make this country stronger, to make it more resilient and to be able to solve the kind
of issues needed to be prepared for the next attack, the next hurricane or the next incident. We don’t know what it is going to be, but believe me, it is going to happen. To the extent that we can create public-private partnerships, we will be so much better off.

Synopsis - Emergent Themes

The public-private partnership examples included in the symposium illustrate the importance and strong benefits of collaboration among government, private industry, and academia in addressing homeland security challenges. Some important common themes were reinforced by the panels relating to establishment and operation of public-private partnerships and their benefits in improving system and community resilience.

3. Public-private partnerships reap benefits at all levels, federal, state, and local.

4. Bringing state government, business, and academic communities together has resulted in much better informed and comprehensive planning for regional emergency preparedness.

5. Public-private partnerships provide mutual, win-win benefits to the public and private sectors. Examples were given illustrating the private sector becoming a “force multiplier” for the public sector. The public sector helps the business continuity of the private sector.

6. Outcomes are both people-driven and process-driven. It is helpful to have goals and metrics related to the outcomes.

7. Public-private partnerships result in cost savings.

8. Public-private partnerships are not easy to establish and sustain. The key is finding where public interests lie and where private interests lie and then finding common ground. The private sector participates in three roles: as a victim, vendor, and partner. The partner role is the most challenging.

9. Public-private partnerships require mutual trust, a common objective, and organization skills to get people and groups to work together over the long periods needed to solve homeland security problems. Relationships need to be based on mutual benefit and respect rather than being externally forced. A culture of collaboration is essential and the partnership needs to build it, sustain it, and take pride in it.

10. Partnerships require sharing resources.

11. Professional societies are often a very important venue for coordination, information exchange between the public and private sectors, and the establishment and life of public-private partnerships.

12. Public-private partnerships require good communication. Partners need to develop a common language that often times is not there to begin with due to differences in communities and disciplines among the participants.

13. Information sensitivity is a major hurdle in establishing public-private partnerships. Means must be developed to protect critical private sector information from disclosure.

14. Partnerships work when participants recognize that their citizenship extends far beyond narrow self-interest.

15. Public-private partnerships benefit from including academia at the table. Modest funding can reap major benefits due to the intellectual capital that is brought to bear.
For further information on the symposium or to request proceedings, please visit: