

James Madison University

From the Selected Works of George H Baker

Spring 2009

Homeland Security: Fostering Public-Private Partnerships

George H Baker, *James Madison University*

Cheryl J Elliott, *James Madison University*



Available at: https://works.bepress.com/george_h_baker/24/

2008 Proceedings

Version 4/20/2009



Institute for Infrastructure and Information Assurance
at James Madison University

- in cooperation with the -

National Academies'
Federal Facilities Council

- presents -

2008 Homeland Security Symposium Fostering Public-Private Partnerships

Thursday, May 22, 2008, National Academies, Washington DC
www.jmu.edu/iiia/2008symposium



Proceedings
of the
Institute for Infrastructure & Information Assurance
and the
Federal Facilities Council of the National Academies

2008 Homeland Security Symposium Fostering Public-Private Partnerships

**The National Academy of Sciences
2100 C Street, N.W.
Washington, D.C.**

May 22, 2008

George H. Baker
Cheryl J. Elliott
Editors

Institute for Infrastructure & Information Assurance
James Madison University, Harrisonburg, Virginia
© 2009 IIIA Publication 09-01



James Madison University partners with George Mason University on the Critical Infrastructure Protection Program (CIPP).

This research was supported [in part] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.

Edited by George H. Baker and Cheryl J. Elliott

Graphic Design by Cheryl J. Elliott

Proceedings by: CASET Associates, Ltd., 10201 Lee Highway, Fairfax, Virginia 22030 (703)352-0091

Limited copies are available from the Institute for Infrastructure & Information Assurance (IIIA), 800 South Main Street, MSC 3804, Harrisonburg, VA 22807; 540-568-4442. This publication is available electronically on the website: www.jmu.edu/iiia/

IIIA Publication 09-01

Copyright © 2009. The Institute for Infrastructure & Information Assurance at James Madison University, Harrisonburg, Virginia, USA and the Individual Authors. ALL RIGHTS RESERVED. No part of this publication may be reproduced, stored in any retrieval system, or transmitted in any form or by any means - electronic, mechanical, digital, photocopy, recording, or any other - except for brief quotations in printed reviews, without the prior explicit written permission of the publisher, editors or respective author(s).

Printed in the U.S.A. Printed by Mid Valley Press, Verona, Virginia

Section	Page
Introduction to the 2008 Symposium	1
Section I: Symposium Themes	
Emergent Themes	4
Executive Summary	5-11
Section II: Symposium Event	
Event Schedule	14-16
Homeland Security Efforts at JMU	18-19
2008 IIIA Fellows	20-21
Dialogue with IIIA Fellows	22-24
Homeland Security Education at JMU	25
Section III: Symposium Appendices	
A: Transcripts	29-78
B: Presenter Bios	79-86
C: Posters	87-98
About your Hosts	99

The archival webcast of this Symposium is available at <http://media.jmu.edu/archives.asp#Video>. If you have trouble accessing these videos, [please contact](#)

If you are interested in learning more about the research presented today, please contact the presenters directly. If you would like more information on JMU capabilities, please contact Cheryl Elliott (contact information is listed on page 99 of this book).

For more information on IIIA, please visit our website at: <http://www.jmu.edu/iiia>. The proceedings for this event will be posted online on our website at http://www.jmu.edu/iiia/resources/resources_symposiums.html

Over breaks and lunch, participants could visit the Poster Presentations in the Great Hall. Poster Authors were available near their posters. The posters are included here beginning on page 87.

Please read about new and current research activities at JMU on page 18-19. JMU's new Institute for National Security Analysis is described on page 98.

Introduction



Welcome,

On behalf of James Madison University and the Institute for Infrastructure and Information Assurance, I am pleased to welcome you to the 2008 Homeland Security Symposium, *Fostering Public-Private Partnerships*. It is widely accepted that over 80 percent of the nation's critical infrastructure is owned and operated by the private sector. This poses a unique challenge to government organizations charged with providing safety and security to the citizenry.



Public-private partnerships are essential to advancing the efforts to secure our homeland. Well-coordinated partnerships between industry and government bring the full capabilities of industry squarely into the national preparedness and response agenda. Through this symposium, we seek to advance the dialogue on the importance of collaboration by providing examples of successful partnerships across the levels of government. These models highlight how preparedness and response efforts are more effective when organizations work together towards a common goal.

Symposium participants include leaders from academe, federal/state/local government agencies, private-sector companies, industry associations, and standards organizations. This unique cross-section of participants presents an opportunity to learn from existing partnership models and perhaps, more importantly, develop new collaborative relationships.

I would like to thank our host, the National Academies' Federal Facilities Council, and our cooperating partners, The Infrastructure Security Partnership and the American Public Works Association, for their continued support of the symposium. I trust you will find the symposium to be insightful and meaningful.

Sincerely,

A handwritten signature in dark ink, appearing to read "John B. Noftsinger, Jr.", with a stylized flourish at the end.

John B. Noftsinger, Jr.

Vice Provost, James Madison University
Executive Director, IIIA

Section I: Symposium Themes



In this section you will find the Symposium's
Emerging Themes and the Executive Summary.

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.

1 In most cases, solutions to homeland security problems are not possible without public-private partnerships. The fact that most critical infrastructures are privately-owned reinforces this theme. The government does not have the organic technical expertise needed to solve many problems.

2 Public-private partnerships improve the effectiveness of solutions. The private sector brings innovation, management expertise and the profit motive to the table. The government brings authority, management expertise, high-level perspective, and funding to the table. Both are needed to achieve best solutions to homeland security problems.

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, and 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 oftentimes 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 the academic sector at the table. Modest funding can reap major benefits due to the intellectual capital that is brought to bear.

To foster the development of public-private-partnerships, JMU in cooperation with the Federal Facilities Council of the National Research Council organized a symposium held on May 22nd, 2008 at the National Academy of Sciences. Cooperating partners included The Infrastructure Security Partnership (TISP) and the American Public Works Association (APWA).

The theme of this 3rd annual JMU/FFC Homeland Security Symposium, Fostering Public-Private Partnerships, was based on an important conclusion from our 2007 symposium whose theme was 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 the 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 Honoré, who led the National Guard response to Katrina has 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 academe, Federal/State/Local government agencies, private-sector companies, industry associations, and standards organizations.

Symposium Morning Keynote

Congressman Dutch Ruppersberger, Maryland 2nd District, emphasized the importance of government-industry partnerships but also stressed the importance of academe in solving homeland security problems. His district relies heavily on expertise of Johns Hopkins University, the University of Maryland and Towson

University. His talk focused on two technical areas in need of improved public-private partnership: 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. But 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 enterprise is mostly privately owned and controlled. Both areas require strong partnerships between government industry and academe if our national security is to be protected.

A major source of US 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 timelines 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 shortfalls are worrisome given the challenges posed by Russia and China.

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

Congress is responsible as well. Having experienced problems with committee processes, Congressman Ruppersberger has instituted “tabletop meetings,” which allow for more time to complex procurement problems. The tabletop format in the Intelligence Committee has helped greatly with problem solving.

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,

Executive Summary

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 a bank run unlike anything we've seen in the past. Financial markets would panic. Even if the network were only down for a day there could be catastrophic consequences for our economy.

It is important to note that Russia knows how to take down the web of an entire country and did so in Estonia. They targeted and took down Estonia's financial networks. The attacks were traced back to Russian communication agency. Admittedly, Estonia is a small country of 1.4 million. Regardless, these attacks show that it is all too easy to use basic Internet hacking techniques to wreak havoc with a nation's information infrastructure.

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.

Government and industry have worked together to make our nation more secure for more than a century. We have brand-new challenges facing us in cybersecurity, and our traditional dominance in the world of satellites and overhead architecture is threatened by other nations. We cannot take our eye off the ball, especially watching China and Russia. But I have every confidence that we as Americans by working together, by educating our students, we will meet these challenges and keep our country the strongest in the world.

Congressman C.A. “Dutch” Ruppberger, 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. He was the first Democratic freshman ever to be appointed to the House Select Committee on Intelligence. The committee oversees the collection and analysis of intelligence information from all around the world to ensure our national security and prevent potential crisis situations – especially terrorist activity.

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

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. Local/state/federal 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.

From its initial planning meeting with members of the American Society for Industrial Security (ASIS) local chapter, SPIN has been a true partnership, valuing the importance of collaboration and working together towards a shared public-private vision. Enlisting the help of nearly two dozen sector-specific organizations – including groups such as the Long Island College and University Security Consortium and the New York State Self Storage Association – the network has grown exponentially from just 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.

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 resulting relationships have helped facilitate cooperation and coordination in emergency preparedness and planning, and have contributed to making Nassau County a safer place.

The development of SPIN has provided major benefits related to crime prevention and response, business continuity, and homeland security in Nassau County, New York. Lessons learned from this partnership process include the importance of involving professional societies such as ASIS for coordination and information exchange between the public and private sectors; the use of focus groups to define information needs for partnership; private sector involvement broke down the information sensitivity “walls of silence;” mutual respect and trust between public and private partners has been essential to sustaining long term relationships; and the use of existing software tools (SPIN uses Microsoft Outlook) for network operation and information sharing keeps the costs reasonable.

Panelists: Assistant Chief ____ Tully, Nassau County Police Department, Moderator; Detective Sergeant William Leahy, SPIN Coordinator, Homeland Security and Counter Terrorism Bureau, Nassau County Police Department; Oksana Farber, insurance industry professional; Mr. Mario Doyle, Director of the Police Reserve Force for Nassau County.

PANEL 2 – Regional Public-Private Partnership: Mid-Atlantic States All Hazards Consortium

The All Hazards Consortium (AHC) is an example of a regional public-private partnership. The AHC was formed to create a multi-state network of people from homeland security stakeholder groups within government, the private sector, universities and non-profit organizations. It spans nine states in the Mid-Atlantic region. The consortium acts as a facilitator to bring the stakeholders together from across the region to share information, collaborate in addressing possible solutions to regional homeland security challenges, identify funding sources, and develop regional initiatives that produce results.

The All Hazards Consortium was built on the belief that state/local 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 needs), a powerful environment for collaboration is created to solve tough problems that require resources from every sector.

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 the workshop deliberations, the AHC produces white papers with recommendations to be shared with federal agencies and cognizant Congressional staff. The white papers’ recommendations form the basis for multi-jurisdictional funding proposals. Workshop topics (and subsequent white papers) have included interoperability, catastrophic evacuation planning, fusion centers, and critical infrastructure protection. In July 2008, the consortium is sponsoring a GIS workshop at Towson.

The AHC began as an event (All Hazards Forum) and grew into an organization (All Hazards Consortium). As the event gained momentum, it became clear that follow-up actions were needed to implement what was learned. In the last 18 months, workshops have further coordinated and implemented partnership decisions on a continuing basis.

The objective of the AHC is improved regional readiness. An important function of the consortium is to get leaders involved with practitioners and find the right people to work identified problems. The consortium 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 twenty region-level homeland security and emergency management issues that the member states have identified.

Public-private partnerships are not easy to implement. 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.

The Role of Academia

Higher ed’s role in the AHC includes education, research, community outreach, and government service. Often the mission of higher ed is only seen as training, but research dollars is what gets attention behind the ivy doors. With homeland security efforts the challenge is to find rapid solutions because years

Executive Summary

of research are not possible. Universities are often affordable; modest funding can reap major benefits due to the intellectual capital available. The AHC allows higher ed to get in touch with the people owning the problems, figuring out who has the necessary resources, and how collaborations for solutions can be created. Listening and learning is a challenge and takes a lot of patience and one-on-one engagement.

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. Northrop Grumman sees AHC as an extension of their marketing communications efforts, enhancing existing and new information-sharing relationships. The consortium 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 won't stay engaged. As long as we stay focused on the problem and maintain trust amongst the parties, we can work collaboratively and engagingly. When either of those two tenets is violated, there will be problems.

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

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

The President's National Security Telecommunications Advisory Committee (NSTAC) has a 25-year history of Industry-Government partnership with several important contributions to

assure the security of the Nations telecommunications service. Recently, the 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 national 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 experts from the telecom, electric power industries and government subject matter experts 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 government Communications Dependency on Electric Power Working Group (CDEP WG) in response.

Mr. Dan Hurley chairs the Electric Power Communications Dependency on Electric Power (CDEP) Working Group. Their 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. They are also looking at new technologies for backup power including fuel cells, wind power, photovoltaics, and recovery transformers. The working group should have an initial draft report on their findings by end of the summer 2008.

NSTAC industry subcommittees are ongoing and productive. The government supports the NSTAC primarily by providing information. Government representatives don't get involved in deliberations. Some examples of areas being addressed by the 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 systems “SCADA.” Mr. Ackerman asked two fundamental questions: (1) how do the telecom 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 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 telecom industry to include members of the electric power and other private industry and government organizations in the U.S. and Canada. In North America there is no distinction between Canada and the U.S. in electric power and telecom. However, there are big differences in viewpoint 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 the large scale outages.

The 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.

Panelists: Dr. John S. Edwards, Nortel’s Designated Representative to the NSTAC’s Industry Executive Subcommittee, Moderator; Mr. 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 (CDEP) Working Group; Mr. Lawrence Hale, Acting Director of National Communication System (NCS).

Symposium Afternoon Keynote

As Assistant Secretary for the Private Sector Office of DHS, Secretary Martinez-Fonts described the 2002 law that created the Department of Homeland Security which also gave his office seven tasks to achieve. Subsequent laws over the last five plus years have added four more tasks, bringing the total to 11 different things. Four of these are what he considers to be key.

First and foremost, we are an advocate for the private sector. If you are in the private sector, I’m the guy you want to know in the Department, among many other people. I don’t have a budget, I don’t buy things, and I’m not on the procurement side. My job is to advocate clearly on strategic issues. We work on getting people in and out of the country, and getting goods, trade, in and out of the country. We work on issues that are very broad ranging that affect the private sector including presenting the views of the private sector to the Secretary. Examples of current issues affecting the private sector are real ID and the Western Hemisphere travel initiative.

The second thing that we do is share information and best practices. I don’t generate 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.

We have done a lot of work getting information out on best practices. One area of particular emphasis is pandemic influenza. I had the opportunity to participate in meetings with Secretary Leavitt and talk about what needs to be done. Secretary Leavitt in HHS is very much concerned about the sick and the dying in the event of a pandemic. He wants to make sure we have the vaccines, the antivirals, the respirators, et cetera that we need. We want to make sure that hospitals have the electricity, water, food and necessary transportation to deliver supplies. We want to make sure that the critical infrastructure is working in a pan flu contingency.

One practice of high interest is telecommuting. In a pan flu situation, many people can avoid contact by performing their jobs in telecommute mode. Of course, this is not possible if you are running a steel plant or assembling cars in a General Motors plant. But a lot of businesses can operate by telecommuting. An insurance company in Boston learned got some important clues on telecommuting by asking a good-sized corporate audience of how many of them ever asked their employees what kind of computers they have at home and how they connect to the Internet. In the course of the follow-up, they found that 22 percent of their people have 386 or 486 chips in their computer and that 50 percent use dialup Internet access. Companies will need to address these shortfalls in the course of establishing telecommuting capabilities.

Executive Summary

Regarding economic consequences, my department employs largest number (seven) of economists of any office in DHS to look at the economic consequences of homeland security, from both the micro and macro economic perspectives. From the micro side we might look at containers coming in from Taiwan with sneakers that have a 15 cent lead seal on them with a series of numbers that we deem not to be very efficient or effective. One option to improve effectiveness would be to enlist the private sector to develop a lock RFID temperature humidity sensor with a global positioning system that is tamper resistant but costs \$5,000. If we go this route, your sneakers from Taiwan are going to cost a lot more. We must weigh the alternatives in terms of cost-benefit.

We have performed macro-economic analysis mostly in connection with exercises. For example, what happens if a 20-kiloton bomb explodes in the port of L.A.-Long Beach? What are the effects on the economy? What gets hurt?

In the Private Sector Office, public-private partnerships are clearly the cornerstone of our mission. Many of you may know Jan Meiers who is my deputy. Jan could not get into a school like I went to, Villanova, so he went to Harvard as an undergraduate, then to MIT for his masters in chemical engineering, and then back to Harvard for law school. Jan wrote a great paper last year on public-private partnerships that he presented at a symposium in Europe. One of his main themes is that we really need to have the two sides present in solving homeland security problems. And it is essential to have a common goal.

In public-private partnerships, there is a need for a champion... someone who will sometimes put their 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 CTPAT, 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 people 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 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, no one 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 most importantly the industry sector and the government. CIPAC created that protective space to do 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

In my office, I like to think of myself and what we do as being an inch deep and a mile wide. We cut across every single industry – the corner dry cleaner and the nuclear power plant operator are my customers. Bob Stephan integrates all 18 sectors, and he also is an inch wide and a mile deep. He can reach every single nuclear power plant in the United States, in theory every single bank, in theory every single eating and food establishment, and so on. This is important because high consequence events happen in a place.

I am a huge believer in all of us working together. I spent 30 years in the private sector. I must admit that every time the government called me up I worried that they were going to demand something, ask me to do something, or spend some money. Now that I am in the government, I talk to people who have been their whole careers in the government and they say, those people from the private sector, they are just pushing a product or trying to get your dollars. Let me just tell you, both

reactions are wrong. There are many wonderful people in the private sector who have real commitment to making this country safe and secure. Likewise, there are some fabulous people in the government who understand that we need to protect the private sector and are willing to go above and beyond the call of duty to do this.

Being able to create those two 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 kinds 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.

The Honorable Alfonso "Al" Martinez-Fonts, Jr., is Assistant Secretary for the Private Sector Office, Department of Homeland Security. His mission is to provide our private sector with a direct line of communication to the Department of Homeland Security. His office works directly with individual companies and trade associations to foster public-private policy dialogue and partnerships. He has a distinguished career both in government and the private sector. His private sector experience is in the banking sector. Before coming to the Department of Homeland Security, he was chairman and CEO of J.P. Morgan Chase Bank in El Paso, Texas, and prior to that he gained much international experience by managing offices in the Philippines, Mexico City, Argentina, Chile, Uruguay, Paraguay and Bolivia for the Chemical Bank.

Section II: Symposium Event



In this section you will find the details from the event, including the day's schedule, information about JMU's programs and research efforts.

Thursday, May 22, 2008 @ National Academy of Sciences

8:00-8:30 a.m.	Continental Breakfast (Registration and Networking)
8:30-8:50	<p>Welcome and Symposium Introduction</p> <p>Master of Ceremonies: Mr. Steve C. Knickrehm, Associate Director for Policy, IIIA</p> <p>Lynda Stanley, Federal Facilities Council, NAS</p> <p>Dr. John B. Noftsinger, Jr., Vice Provost and Executive Director IIIA</p> <p>Dr. Linwood Rose, President, James Madison University</p>
8:50-9:30	<p>Keynote Presentation 1 -- Congressman C.A. Dutch Ruppersberger, Maryland</p> <p>Introduction by Dr. Linwood Rose</p>
9:30-9:45	Break in the Great Hall (Poster Authors Available)
9:45-11:15 a.m.	<p>Panel One: Nassau County Security/Police Information Network Local Panel</p> <p>Moderator: Inspector Matthew J. Simeone, Jr., Moderator, former SPIN Administrator, Nassau County Police Department</p> <p>The Security/Police Information Network (SPIN) is a virtual public-private partnership (VP3) that seeks to increase public safety through the sharing of important and timely information. Created by the Nassau County Police Department in 2004, SPIN utilizes email 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 also enabled the police department to leverage the private sector in order to prevent crime, arrest offenders, and otherwise maintain safer communities.</p> <p>From its initial planning meeting with members of the local ASIS International chapter, SPIN has been a true partnership valuing the importance of collaboration and working together towards a shared public-private vision. Enlisting the help of nearly two dozen sector-specific organizations – including groups such as the Long Island College and University Security Consortium and the New York State Self Storage Association – the network has grown exponentially from just 175 security directors at its inception, to approximately 800 security directors and personnel from nearly every sector and critical infrastructure, nearly 200 business and community leaders, 100 government employees, and over 400 members of federal, state, and local law enforcement.</p> <p>Taking an “all-crimes, all-threats, all-hazards” approach to information sharing, SPIN’s content is wide ranging – 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 resulting relationships have helped facilitate cooperation and coordination in emergency preparedness and planning, and have contributed to making Nassau County a safer place.</p> <p>This panel will discuss SPIN’s beginnings, its development, its successes, and its challenges. In addition, the panel will explore the dynamics of the public-private partnership and its impact on crime, business continuity, and homeland security in Nassau County, New York.</p> <p>Panelists:</p> <p>Ms. Oksana Farber, Vice President of Operations, Hiram Cohen & Son, Inc.</p> <p>Vice Chair, Law Enforcement Liaison Council, ASIS International</p> <p>Mr. Mario Doyle, CPP, Vice President, BuildingStar Security Corporation, Regional Vice President, ASIS International</p> <p>Detective Sergeant William Leahy, SPIN Coordinator, Homeland Security and Counter Terrorism Bureau, Nassau County Police Department</p>

11:15-11:30	Break in the Great Hall (Poster Authors Available)
11:30-1:00 p.m.	<p>Panel Two: All Hazards Consortium (Regional) Panel</p> <p>Moderator: Mr. Robert Crouch (Assistant to the Governor for Commonwealth Preparedness, Virginia)</p> <p>The All Hazards Consortium (AHC) is a Maryland nonprofit charitable organization, guided by the regional states of NC, DC, MD, VA, WV, DE, PA, NJ and NY. Our mission is to help create new resources and funding opportunities for the states to support regional multi-state collaboration efforts among our stakeholders from government, private sector, higher education and non-profit/volunteer organizations.</p> <p>The All Hazards Consortium was built on the belief that state/local 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 needs), a powerful environment for collaboration is created to solve tough problems that require resources from every sector.</p> <p>This “culture of collaboration” is what creates the energy that drives the All Hazards Consortium and its supporters to work together to protect the region’s citizens from all types of hazards. This panel will discuss the partnership relationship: who we are, whom we serve and how, and tangible accomplishments of the Consortium.</p> <p>Panelists:</p> <p>University rep Dave Lindstrom (Penn State University)</p> <p>Government rep John Contestabile (Maryland)</p> <p>Private Sector rep Michael Hughes (Northrop Grumman Corporation)</p> <p>Executive Director Tom Moran (All Hazards Consortium)</p>
1:00-1:30 p.m.	Lunch in the Great Hall
1:30-3:00 p.m.	<p>Panel Three: National Security Telecommunications Advisory Committee</p> <p>Telecommunications/Electric Interdependency Panel</p> <p>Moderator: Dr. John S. Edwards, Nortel's Designated Representative to the NSTAC's Industry Executive Subcommittee</p> <p>The President's National Security Telecommunications Advisory Committee (NSTAC) has a 25-year history of Industry-Government partnership with several important contributions to assure the security of the Nations telecommunications service. Recently, the 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 national 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.</p> <p>Both reports were a collaboration among the Telecommunications and Electric Power Industries and the Governments of Canada and the United States. Although the NSTAC, a telecommunications entity sponsored and led the effort, a unique collection of experts from the telecom, electric power industries and government subject matter experts from both countries met collegially over a two-year period.</p> <p><i>Continued next page</i></p>

Schedule

	<p>The reports were submitted to President Bush and as a result, the government established a government Communications Dependency on Electric Power Working Group (CDEP WG) in response.</p> <p>This effort brought together individuals with broad and diverse backgrounds and demonstrated the efficacy of a disciplined approach to the subject. This panel will discuss the partnership relationship and how it was established.</p> <p>Panelists:</p> <p>Mr. Daniel C. Hurley, Jr., Director, Critical Infrastructure Protection, U.S. Department of Commerce, National Telecommunications and Information Administration and Chair of the CDEP WG</p> <p>Mr. Lawrence C. Hale, Acting Director and Chief, Customer Service Division, National Communications System</p>
3:00-3:15 p.m.	Break in the Great Hall (Poster Authors Available)
3:15-4:00 p.m.	<p>Keynote Presentation 2 -- Alfonso "Al" Martinez-Fonts, Jr., Assistant Secretary for the Private Sector Office, Department of Homeland Security</p> <p>Introduction by: Dr. George H. Baker, Technical Director, IIIA</p>
4:00-4:30	<p>Symposium Recap</p> <p>Dr. Jerry Benson, Vice Provost, James Madison University</p> <p>Dr. Robert Reid, Dean, College of Business, James Madison University</p>
4:30	Adjourn

Thank you to our
Cooperating Partners:



The Infrastructure Security
Partnership
www.tisp.org



American Public Works
Association
www.apwa.net

Symposium Emcee -- Steve Knickrehm, Associate Director for Policy, IIIA and Assistant Professor of Health Sciences

Symposium Planning Committee -- Lynda Stanley, George Baker, Steve Knickrehm, Ryan Cornett, and Cheryl Elliott

A special thanks to Becky Rohlf for event organization and Amy Ballard for staff assistance.

Many Thanks...

James Madison University and the Institute for Infrastructure and Information Assurance express our gratitude to the National Academies and the Federal Facilities Council for hosting this event.

Homeland Security Efforts at JMU



Institute
for Infrastructure
and Information Assurance
at James Madison University

Research Summaries

Each year IIA extends invitations to JMU faculty to participate in the annual request for proposals for summer research funding. The projects chosen for funding for the 2008 cycle are as follows:

Efficient End-Use for Energy Security

Energy security starts with efficient end-use and conversion. There is plenty of room. The U.S. throws away 1.2 times as much energy in the form of power plant waste heat as Japan consumes. Efficient use of energy also reduces upstream supply pressures, allows alternative sources to supply a bigger share, and stretches emergency stockpiles, buying time for repairs and substitutions. Monitoring and collecting data from all participants in a local power company's Demand Response and Green Power Rate Programs and analyzing the data is the main objective of our research. A research team of one JMU faculty member and two students is working with Dominion Virginia Power in Richmond, Virginia, in implementing these two programs in the Central Shenandoah Valley. A follow-up of evaluation of these two programs will provide valuable information to the region and our nation's energy security.

Contact: Dr. Tony D. Chen, Dept. of Integrated Science and Technology, James Madison University, chendt@jmu.edu

Hosting a Cyber Defense Competition

Cyber Defense competitions are important and challenging opportunities for participants to test their Information Security knowledge and skills in a realistic environment. Contestants are given a group of machines to administer and defend over a period of 24-48 hours. Teams are scored on their ability to maintain proper functioning of their hosts and avoid compromises by a dedicated team of attackers. JMU participated in the Collegiate Cyber Defense Competition last year, and we plan to participate again this year and in subsequent years. JMU will now benefit greatly by having the ability to host our own Cyber Defense Competitions. We foresee hosting competitions for our own students, for prospective students from around the country, and, perhaps, for local or regional businesses.

Contact: Dr. Brett Tjaden and Dr. M. Hossain Heydari, Dept. of Computer Science, tjadenbc@jmu.edu, heydarmh@jmu.edu

Weapons of Mass Destruction Awareness Training for the City of Harrisonburg and the Rockingham County Fire and Rescue Departments

Weapons of Mass Destruction (WMD) Standardized Awareness Training

(AWR-160) is a FEMA/DHS course that standardizes the minimum WMD awareness level learning objectives that shall be included in all federal, state, and local jurisdictions. This course establishes a common baseline to ensure nationwide consistency in WMD education and training for first responders. The course must be taught by a FEMA/DHS certified instructor. The course will be taught to all fire and rescue personnel in the city of Harrisonburg, and the county of Rockingham. Delivery of the course for the city of Harrisonburg will be done for each of the three shifts, which consist of four engine companies and one truck

Providing policy and technical solutions for cyber and physical security issues facing our nation.

company. Total personnel for each shift are 18, resulting in 54 Harrisonburg Fire and Rescue personnel being certified for the AWR-160 course. Rockingham County presents a geographical problem due to its size. It is impossible to bring all the personnel from one shift together for the class. Thus, the instructor must go to each company and shift to teach the class. There are 11 companies with three shifts with a total of 70 personnel that will receive this certification.

Contact: Dr. Ronald W. Raab, Dept. of Integrated Science and Technology, James Madison University, raabrw@jmu.edu

Toward a Computerized Constructive Cartography and Communication Center

The innovative method of *constructive cartography* is being used to model the spread of disease. Charts are constructed

by computer, based on clinical or epidemiological data, such that disease (or health) spreads in concentric rings across the constructed landscape (depicting our body or Homeland). Various starting places and symptoms of the threat are placed within the constructed map such that nearby sites are likely similar in involvement (to share risk in the case of threat or not to share in the case of spreading safety).

Statistical significance can be evaluated. Results allow interactive predictions of how various threats are spread or are stopped from spreading. Preliminary visualizations can be seen at <http://www.csd.jmu.edu/csdsquared/>. Such charts are, in a sense, the threats' view of the world. These interactive displays aid communication. Otherwise intractably complex patterns are reduced to easily interpretable graphics using this method.

Contact: Dr. Lincoln Gray, Professor of Communications Sciences and Disorders, James Madison University, graylc@jmu.edu

RFID Disaster Identification Bracelet System (DIBS)

On Thursday, September 15, 2005, in the wake of Hurricane Katrina, President George W. Bush addressed the nation in a nationally televised speech describing the aftermath of the powerful storm and outlining a plan for recovery. As tragic as any disastrous hurricane can be, it is often paired with a second potential disaster: a large-scale evacuation that leads to the separation of families and loved ones. According to the Federal Emergency Management Agency (FEMA), after Hurricane Katrina, more than 330,000 families were displaced from their homes. Of these, over 182,000 victims of the storm moved into Red Cross and Salvation Army shelters across more than 20 states. Many

of these individuals were separated from their families and loved ones and remained separated for many weeks.

To address these critical needs, JMU and RFID Informatics, Inc. have partnered to develop a simple cost-effective system that uses Radio Frequency Identification (RFID) technology to track the current location of large numbers of individuals that have been evacuated to shelters in several different geographical locations during a natural disaster. The partnership proposes to use RFID-embedded bracelets that have been registered in a national secure database

and involves automatic tracking and data logging, rapid information retrieval, an effective notification method, and a centralized, secure data storage center that is worldwide accessible. The model system previously developed will serve as a prototype for the development and implementation of a large-scale tracking and notification system to be used during hurricane evacuations with negligible cost or effort on the part of the end-user.

Contact: Dr. Anthony A. Teate, Dept. of Integrated Science and Technology, James Madison University, teatea@jmu.edu

Making a Difference! TECHNOLOGIES AT JMU



A NEW KIND OF RESEARCH UNIVERSITY

JMU's enterprise-wide research agenda is changing the landscape of innovation with cross-disciplinary focus on real-world problems. We enhance our research by connecting inventors and industry to foster economic development.



JAMES MADISON UNIVERSITY
OFFICE of
TECHNOLOGY TRANSFER

Mary Lou Bourne, Director of Technology Transfer
bourneml@jmu.edu (540) 568-2865 or FAX (540) 568-8831
1401 Technology Drive, Room 1122, MSC 4904
James Madison University, Harrisonburg, VA 22807

www.jmu.edu/ott

Accelerating innovation by connecting researchers and industry

2008 IIIA Fellows

The Institute for Infrastructure and Information Assurance welcomes the 2008 class of IIIA Fellows. These researchers have made outstanding contributions to Infrastructure Protection and Information Assurance.

Key criteria for IIIA Fellows include:

- demonstrated significant contributions through scholarship or practice in infrastructure and/or information assurance.
- demonstrated effectiveness as leader and communicator in infrastructure and/or information assurance (including publication).
- demonstrated excellence in and commitment to teaching and mentoring university students.
- proven record of obtaining and managing external research grants.

COL (Ret.) Dennis Barlow

Dennis is a retired U.S. Army Colonel who previously was the Director of Humanitarian Policy in the Office of the Secretary of Defense and the first leader of the Humanitarian Demining Task Force in the Pentagon. He has coordinated civil-military actions with NGOs and the United Nations in Panama, Saudi Arabia, Iraq, Kurdistan and Haiti.

Since 1997, Dennis has served as the Director of the JMU Mine Action Information Center (MAIC). The MAIC at James Madison University is a public policy center which manages information and conducts training relevant to humanitarian mine clearance, victim assistance, mine risk reduction and other landmine-related issues. As an information clearinghouse, the MAIC provides training, operates a help desk for queries, hosts conferences and symposia on landmine-related topics, publishes a journal about mine action, maintains a content-rich web site, develops mine-action education materials, produces global information system (GIS) products and conducts studies and surveys designed to facilitate and improve global landmine action.

Mr. Frank J. Cilluffo

As Associate Vice President for Homeland Security at The George Washington University, Frank J. Cilluffo leads the University's homeland security efforts on education, research, training, and policy <http://www.homelandsecurity.gwu.edu>. He also

directs the multi-disciplinary Homeland Security Policy Institute and teaches a graduate level course on counterterrorism and homeland security at the Elliott School of International Affairs.

Frank joined GWU after leaving the White House, where he served as Special Assistant to the President for Homeland Security. Shortly following the September 11, 2001 terrorist attacks on the United States, Frank was appointed by President George W. Bush to the newly created Office of Homeland Security. In his capacity as Special Assistant to the President for External Affairs, Frank was responsible for engaging and building partnerships with the private sector, academic institutions, state and local officials, and emergency responders concerning homeland security policies and initiatives. He was a principal advisor to Governor Tom Ridge and directed the President's Homeland Security Advisory Council and its four Senior Advisory Committees.

Prior to his White House appointment, Frank spent eight years in senior policy positions with the Center for Strategic and International Studies (CSIS), a Washington based think tank. At CSIS, he chaired or directed numerous committees and task forces on homeland defense, counterterrorism, transnational crime, information warfare, and information assurance.

In addition to publishing extensively in academic, law, business, and policy journals, as well as magazines and newspapers worldwide, Frank is co-author and editor of *Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy* (2001); *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (2001); *Russian Organized Crime & Corruption: Putin's Challenge* (2000); *Cybercrime, Cyberterrorism, Cyberwarfare* (1998); *Russian Organized Crime* (1997); and *Global Organized Crime: The New Empire of Evil* (1994).

He has testified before the United States Congress on a number of occasions and has been a regular guest on major television and radio networks worldwide. Frank presently serves and has served on various national security-related committees sponsored by the U.S. government and non-profit organizations, including the Homeland Security Advisory Council, to which he was appointed by Secretary Tom Ridge.

The Honorable John O. Marsh, Jr.

John O. Marsh, Jr. was born in Winchester, Virginia, in 1926; attended the public schools in Harrisonburg, Virginia; entered the U.S. Army in 1944; was commissioned through the Officer Candidate Course at the Infantry School in 1945; served with the occupation forces in Germany during 1945-47; and was

a member of the United States Army Reserve from 1947-51. He married Glenn Ann Patterson in 1950 and graduated from Washington and Lee University in 1951.

He was admitted to the Virginia State Bar in 1952 and entered the practice of law in Strasburg, Virginia. He served as the town judge of Strasburg and town attorney of New Market, Virginia from 1954-62. He served four terms in the U.S. House of Representatives from Virginia's Seventh District, during 1963-71.

He entered the Army National Guard in Virginia in 1951, graduated from the Army's Airborne Infantry School with a senior parachutist rating in 1964 and retired from Guard service as a lieutenant colonel in 1976.

Marsh was a member of the American Revolution Bicentennial Commission from 1966-70; was Assistant Secretary of Defense for Legislative Affairs from 1973-74; was a counselor to President Gerald R. Ford, 1974-77; and has practiced law with the firm of Mays, Valentine, Davenport, and Moore. He is a member of the Board of Visitors of the Virginia Military Institute.

Marsh served as Secretary of the Army during the years 1981-89, holding the office longer than any previous Secretary. During his tenure, the Army observed the Bicentennial of the founding of the country, implemented the provisions of the Goldwater-Nichols Act making the services more oriented to joint operations, and recognized the Army Staff to eliminate duplication of functions. He is chairman of the Reserve Forces Policy Board.

In addition to leadership positions in national foundations, John Marsh has taught in the areas of cyber-law and national security in various arenas, including the College of William and Mary, George Mason University, and the Virginia Military Institute. Since 1997, he has served as a member of the coordinating committee of the University of Virginia's Critical Incident Analysis Group.

Ms. Lynda Stanley

Ms. Stanley has been the Director of the Board on Infrastructure and the Constructed Environment (BICE) of the National Research Council (NRC) since 2005. The NRC is the operating organization of the National Academies of Sciences and Engineering and the Institute of Medicine. The BICE addresses questions of technology, science, and public policy applied to the relationship between the constructed and natural environments and their interaction with human activities. Lynda served as the Director of the Federal Facilities Council (FFC) of the NRC from 1995-2005. The FFC is a cooperative association of 27 federal

agencies whose mission is to identify and advance technologies, practices, and policy for the improvement of federal facilities from planning through disposal.

At the NRC, Lynda has served as the study director on a series of reports on federal facilities-related issues. These include Stewardship of Federal Facilities: A Proactive Strategy for Protecting the Nation's Public Assets; Outsourcing Management Functions for the Acquisition of Federal Facilities; Investments in Federal Facilities: Asset Management Strategies for the 21st Century; Core Competencies for Federal Facilities Asset Management Through 2020: Transformational Strategies. She has also been involved with the NRC studies on the New Orleans Regional Hurricane Protection Projects, Assessment of the Bureau of Reclamation's Physical Security Program, and Assessment of the Results of External Independent Reviews for U.S. Department of Energy Projects.

Prior to joining the NRC, Lynda was the Director of the Planning Division in Fairfax County, Virginia. She holds a BA in political science and American history from the State University of New York at Albany and a masters in city and regional planning from Harvard University.

The IIIA Fellows

Dr. J. Peter Pham, James Madison University (2006)

Dr. Lennis G. Echterling, James Madison University (2006)

Dr. Massoud Amin, University of Minnesota (2007)

Dr. Michael D. Deaton, James Madison University (2007)

Dr. Mark A. Kirk, University of Virginia (2007)

Dr. Greg B. Saathoff, University of Virginia (2007)

Dr. Frank J. Cilluffo, The George Washington University (2008)

COL (Ret.) Dennis Barlow, James Madison University (2008)

The Honorable John O. Marsh, Jr. (2008)

Ms. Lynda Stanley, National Research Council of the National Academies (2008)

Highlighting the Accomplishments of the IIIA Fellows

In 2-3 sentences, describe the focus on your research, thoughts, efforts over the past year.

Dr. Massoud Amin: My research focuses on two areas: 1) Global transition dynamics to enhance resilience, security and efficiency of complex dynamic systems. These systems include national critical infrastructures for interdependent energy, computer networks, communications, transportation and economic systems. 2) Technology scanning, mapping, and valuation to identify new science and technology-based opportunities that meet the needs and aspirations of today's consumers, companies and the broader society. This thrust builds coherence between short- and longer-term R&D opportunities and their potential impact. More specifically, we have published our work on security of interdependent electric and communication power grids as well as integration of plugin electric hybrid vehicles, utilized as small generators or storage devices, accounting for both dollars and watts.

Dr. Michael D. Deaton: This past year I have focused on three areas of activity: 1) Working with local EMS teams in the Harrisonburg/Rockingham community to evaluate the CATS/HPAC decision support platforms for HAZMAT response. We've conducted a series of tabletop exercises in which utilized the HPAC SCIPUFF atmospheric dispersion model and the ArcGIS® spatial analytical tools to guide EMS personnel in evacuation and decontamination efforts. 2) Exploring the dynamics impacting emergency medical response during large-scale chemical events. Dr. Mark Kirk and I have published on this and have outlined the potential to using Toxic Syndromes as a diagnostic tool to streamline operations and maximize safety impacts during such an event. (See Kirk and Deaton (2007). Bringing Order Out of Chaos: Effective Strategies for Medical Response to Mass Chemical Exposure. *Emergency Med Clin N Am*, 25(2), 527-548). 3) Using system dynamics modeling techniques to evaluate management strategies for maintaining critical infrastructures. My graduate student Patsy Salyers worked with a southern Virginia community to build a model for evaluating the impact of management strategies on the physical integrity of a county-wide water supply system over a 50 year period. (Salyers (2006) *Water Shortages and Water Management in Big Stone Gap, VA: A System Dynamics Analysis*. Master's thesis, Integrated Science and Technology, James Madison University).

Dr. Lennie G. Echterling: During the past year, I have been particularly involved in crisis counseling and follow-up consultation with the survivors of the April 16 Virginia Tech shootings. One research project includes in-depth interviews of Virginia Tech faculty and staff members regarding the factors that have promoted personal and community resilience in response to the catastrophic event. I have also been providing crisis intervention training to volunteers and helping professionals in various parts of the United States and Canada.

Dr. Mark A. Kirk: In March 2008, I joined the Department of Homeland Security, working for the Office of Health Affairs' Assistant Secretary as his Special Advisor for Chemical Defense and Medical Toxicology. I am on Intergovernmental Personnel Act (IPA) assignment from the University of Virginia, where I am Associate Professor in the School of Medicine's Department of Emergency Medicine.

Dr. J. Peter Pham: Since the February 2007 announcement that the United States would stand up a new Department of Defense unified combatant command to focus efforts at achieving substantial diplomatic and security results for both America and her partners in Africa—a region of immense strategic significance not only in the struggle against extremism, but also in our quest for energy security as well as the search for sustainable global development, as my IIIA-supported research pointed out several years ago—I have been quite involved in many facets of the initiative. In addition to tracking the development of AFRICOM, studying the relevant issues from an academic perspective, and publishing my findings, I have also served in a number of advisory roles to the Pentagon and other agencies as well as testified before the U.S. Congress on several occasions. At the invitation of AFRICOM's commander, General William E. "Kip" Ward, I will be giving the keynote address at an off-site retreat for his senior staff.

Dr. Greg Saathoff: Over the past year, I have expanded upon my work on the issue of "home-grown" and prison radicalization. Specifically I testified before the U.S. Commission on Civil Rights and coordinated meetings in London and Riyadh with representatives from eleven governments. In addition, I coordinated a conference on cyber incursions, with participants from the Middle East, Europe and Asia. Speakers included current FBI Director Robert Mueller and former Secretary of Defense James Schlesinger.

Given the Symposium's topic of private-public partnerships, how does your work address this important aspect of protecting and preparing our nation?

Dr. Massoud Amin: While interdisciplinary and self-sufficient centers that cut across schools and departmental boundaries may not be the norm in academia, they are an important part of bridging across disciplines, while connecting to industry, business and government partners. In the Center for the Development of Technological Leadership (CDTL), we work closely with 250 private and public enterprises, focusing on the two areas indicated above. Most of our work is on leveraging technology to have security, quality of life, and business development.

Dr. Michael D. Deaton: Our work with local EMS, medical emergency personnel, and Big Stone Gap, VA are all based on strong partnerships between the academic and local government. Such collaborations are essential for making progress in this important area.

Dr. Lennie G. Echterling: A neglected part of national preparedness is the need to enhance our psychological sense of community. Private-public partnerships are much more likely to be successful if they are based on the principle of interdependence. We need to promote national resolve by affirming our social fabric that can unite us. Instead of attempting to use only fear to goad citizens into preparing for natural disasters and acts of terrorism, we can also promote positive emotions, such as compassion and hope, to foster a collaborative and collective response.

Dr. Mark A. Kirk: My prior work focused on enhancing communications among local, regional and state response agencies. My current DHS role offers me an opportunity to include federal agencies in the communications network that begins at the local level.

Dr. J. Peter Pham: As I argued in several studies over the course of the last year, AFRICOM is more than an internal Pentagon reshuffling. It involves a radical rethinking of 21st century security away from the traditional focus on fighting and winning wars and on building stability through knowledge and development. This approach necessarily involves a partnership between the public and private sectors, not only in operational implementation, but also in creating the conditions necessary for threat prevention and security cooperation.

Dr. Greg Saathoff: Our community shielding concept requires collaborative efforts between the public and private sector. We hope to expand upon our work accomplished within the National Capital Region through prior projects with the Department of Homeland Security and the Office of the Secretary of Defense.

Also, I have been asked to coordinate a major symposium on the phenomenon of "Suicide by Cop." Because of its relationship to workplace violence, this is an important topic that relates to critical incidents and the public/private sector interface.

When thinking about the state of our nation, which thoughts keep you up at night? What topics, research needs, problems, etc. might be your next focus?

Dr. Massoud Amin: There are many persisting critical infrastructure security and national competitiveness challenges, requiring solutions using science and engineering combined with the "human element" at the intersection of technology, innovation, management, policy and leadership. The lack of investment in critical infrastructure and the human capital that maintains, manages and operates these systems are major challenges, as well as lack of incentives for innovation to strategically enhance the security beyond guards, dogs, cameras and guns. A balanced, risk-managed all-hazards approach to the evolving spectra of threats and vulnerabilities is needed, at a cost our nation can afford. Moreover, high-impact challenges posed by complex systems in nature, society, business and technology constitute ideal foci for the shared visions to move these tools techniques and simulations from the laboratory to the marketplace. We can, and we must, transform our critical infrastructure into secure and efficient systems to support the 21st Century digital economy for our nation.

Dr. Michael D. Deaton: I still worry a great deal about the vulnerability of our chemical facilities and the potential for catastrophic failures from hostile action. I am also very interested and concerned in the need for a system-thinking framework for addressing critical infrastructure protection. My work in system dynamics is at least partly geared to addressing this concern.

Dr. Lennie G. Echterling: I have been both inspired and intrigued by the tremendous resilience I have encountered in my crisis counseling work and research interviews. The many

Continued on next page

Dialogue with IIIA Fellows

Continued from page 19

examples of quiet heroism, heart-felt commitment to addressing the needs of others, and profound sense of hope that I have witnessed in my work have kept me up at night--humbled by the dedication and determination of survivors, but also curious about their amazing ability to achieve posttraumatic growth.

Dr. Mark Kirk: We must move preparedness from a government and public service responsibility to a personal responsibility. I am concerned that, as a nation, we are still complacent about preparedness. We need to develop a culture of preparedness.

Dr. J. Peter Pham: The single most disturbing national security issue for me is the fact that even at this late point in the global struggle against terrorists and other extremists who threaten America and her allies, there are some who are still in denial of the strategic challenge we face. With recognition of reality in which we live, we cannot expect to marshal the will, potential, and dynamism which are our society's greatest strength.

Dr. Greg Saathoff: The most challenging threats involve the potential for WMD strikes against the U.S., particularly in the area of nuclear and bio threats. In addition, the cyber threat is more pronounced, as we learn that traditional perimeter firewall approaches are not successful. Our ability to track down perpetrators is extremely limited, thus making effective response often a moot issue.

Information Security

The Graduate InfoSec program at James Madison University is designed for working professionals. The program is delivered to students through the Internet without the frustration of commute and traffic to and from on-campus classrooms. JMU InfoSec provides professional development and research opportunities for those currently employed or interested in information security or infrastructure protection positions in both the government and private industry. The program is attuned to the rapid advances in our information society and incorporates new technologies and laws into the program curriculum.

JMU Information Security educational objectives center on the following areas:

- Computer Security
- Network and Web Security
- Cryptography
- Distributed Network Security
- Assurance and Secure Operations
- Intrusion Detection (recovery and response)
- Cyber Ethics and Law
- Computer Forensics
- Software Assurance

or more information about the **Graduate InfoSec program**, contact Dr. M. Hossain Heydari, Associate Director for Information Assurance, IIIA, 540-568-8745; heydarmh@jmu.edu



Information Analysis

The B.S. in Information Analysis was created specifically for students who want to become intelligence analysts (in either government or private industry). It will uniquely equip students to engage unrecognized, complex, and multidimensional challenges with innovative, rigorous, and transdisciplinary methods to produce proactive, reliable, and integrated solutions. Students will learn to employ an innovative and integrated new information-centric approach to problem-solving by adept navigation through the expanding complex network of data, information, knowledge, and understanding. At each step, students will be enabled to employ four major skill sets to help you become a complete, versatile, and highly desirable employee:



- Cognitive Skill Set (Advanced Critical Thinking and Reasoning: Hypothesis Testing, Causal Analysis, Counterfactual Reasoning, and Strategy Assessment),
- Computational Skill Set (Integration of Technological Tools: Data Mining, Data Modeling, Dynamic Systems Modeling, Information Visualization, Simulation, and Knowledge Discovery),
- Communicative Skill Set (Interpersonal Skills: Oral and Written Communication, Teamwork, Leadership, and Ethical/Legal Reasoning.),
- Contextual Skill Set (Two Options for Two Career Paths):
 - Option One: National Security Track. Social, Political, and Cultural Insight; Ethnic, Religious, and Linguistic Group Analysis; International Security Assessment; National Political Assessment; and Geographic Analysis.
 - Option Two: Competitive Intelligence Track. Economic, Market, and Managerial Understanding; Economic Analysis; Database Management; Market Assessment; and Global Business Strategy.

Students also have the opportunity to develop a customized Subject-Matter Specialty to equip you to address a major national security threat, business challenge, or geographic area. Everything will be based on a foundational understanding of the structure and process of the current Intelligence Community (in both government and private industry).

For more information about the **Information Analysis program**, please contact Dr. Joe Marchal, Director, Information Analysis Program, James Madison University, 540.568.2727; marchajh@jmu.edu

Section III: Symposium Appendices



In this section you will find the Symposium transcripts, presenter bios, and research posters.

Welcome and Symposium Introduction

MR. KNICKREHM: Good morning, everybody. My name is Steve Knickrehm. I am with James Madison University and the Institute for Infrastructure and Information Assurance. I will be your master of ceremonies for today's event.

First on the agenda is the welcome from the two host organizations. Ms. Lynda Stanley, Director of the Federal Facilities Council and part of the National Academies, is our host for this wonderful venue that we have had for the third year in a row, and we thank Lynda very much for that. She will be followed by Dr. John Noftsinger. Dr. Noftsinger is the Vice Provost for Research and Public Service at James Madison University, and also the Executive Director of the Institute.

Remarks by Ms. Lynda Stanley

MS. STANLEY: Thank you, Steve, and thank you – everyone from James Madison.

This is the third symposium that has been cosponsored by James Madison University and the Federal Facilities Council (FFC). Today's theme is all about partnerships. We have a very good partnership here with James Madison and the FFC.

We are talking about building partnerships and doing that in a practical way, as opposed to a theoretical way. That is what we believe we have accomplished working here with James Madison. We hope, and you will see from the list of who is here, that we are bringing together people from academia, from the government at all levels, federal, state and local, the private sector, and even nonprofit such as the FFC. So we are anticipating a very rich dialogue, a really good opportunity for people to share their experience and to really learn from each other and hopefully come up with some better ideas on how to attack or to approach some of the common issues that we all face.

Partnerships are really the basis for the Federal Facilities Council here. The Council started 50 years ago in 1953, when four or five agencies, the General Services Administration, the Army Corps of Engineers, the Navy, and the State Department, got together and said, "We have a lot of the same issues, we are doing a lot of the same research, and we are looking at the same problems. If we collaborate, it might be to the benefit of everybody." That is what we still do.

Now we are supported by 26 federal agencies. They meet on a regular basis. They share information and they also pool their resources – both their intellectual power and their dollars. So when we get everybody together and we look at our budget, the group decides on how they will allocate their resources.

One of the things that we do is to organize symposia like this one. We also develop reports and perform various kinds of studies. You will find these listed on our website, which is for the National Academies Press. We have performed a lot of studies.

The Federal Facilities Council has been involved in homeland security issues for a long time. They published a study in 1988 on protecting federal buildings from terrorism, which talked about not having day care centers in federal buildings, long before the Murrah Center attack. We have been on the cutting edge in a lot of ways in terms of homeland security.

With that, I would like to say thank you again for being here. We have a tremendous agenda here today, lots to be learned. We hope to take advantage of that both in terms of the presentations and in the networking opportunities.

Remarks by Dr. John Noftsinger

DR. NOFTSINGER: Good morning. It is my pleasure to add my welcome to our third symposium. We are very pleased to have this unique relationship between James Madison University and the Federal Facilities Council of the National Academies. I would like to give particular thanks again to Lynda Stanley, our gracious host, for making the venue available.

We appreciate all the support Lynda and her staff have provided. It has actually been very rewarding, and meaningful relationship between the National Academies and James Madison. At this time I would also like to thank the members of the IIIA staff for their assistance: George Baker, Amy Ballard, Ryan Cornett, Cheryl Elliott, Steve Knickrehm, Ken Newbold, Becky Roth, Hussein Heydari, Ben Delp and Patricia Higgins, for their guidance and vision to make the symposium a success. I work with these people every day, and I am amazed and thrilled at how hard they work. We begin the work for next year's symposium next week. They have worked on this for an entire year, and they take great delight in bringing this program together for your benefit.

Recent high-consequence events in the U.S. have made clear the importance of government collaboration with industry. The benefits of such collaborations were clearly seen as lessons from Hurricanes Rita and Katrina. The resources owned and controlled by American industry dwarf those available to local, state and even federal agencies. 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.

As discussed at last year's symposium in the remarks by General Russell Honoré, who led the National Guard's response to Katrina, we need partnering between local, state and federal governments. General Honoré stressed that the biggest part should be played industry, because people in industry, if they understand problems, can take them as a business opportunities. I can't say it with quite the style General Honoré did, but the message is the same.

The Institute for Infrastructure and Information Assurance at James Madison, in cooperation with our partners at George Mason University and the Critical Infrastructure Protection Project, integrates and supports our university efforts in the

increasingly vital area of homeland security. IIIA or “3IA,” as we call it, actively seeks research sponsorship and provides funding for innovative research within the broad context of improving the nation’s security. Providing better balance between physical and cyber security is one of the main goals, as well as combining policy and technological solutions to the security issues facing our nation. JMU is currently collaborating on this endeavor with George Mason and a number of other universities.

Last night we recognized several outstanding individuals who make up our class of 2008 IIIA Fellows. They include -- and if they are here, I would like to ask them to stand -- Lynda Stanley from the National Academies and the Honorable John O. Marsh, former Congressman and Secretary of the Army. I do want to say that Jack Marsh has been instrumental in bringing George Mason and James Madison together. It was his leadership and his vision and his prodding, if you will, to make sure that we work creatively and fairly together, that has kept this partnership together over the last five years. We thank him for that.

Frank Ciluffo from George Washington University and Colonel Dennis Barlow, Director of James Madison University’s Mine Action Center, round out our fellows from the 2008 class. They will be a great addition to our current group of Fellows: Lennie Echterling, Peter Pham, Massoud Amin, Greg Saatoft, Mark Kirk and Mike Deaton.

Our Fellows program was established to cultivate a distinguished group of homeland security leaders from government, academia and nonprofit sectors. The Fellows participate in conversations with government officials, collaborate with the leaders in the national security arena and the IIIA research community at large to publish papers and pursue cooperative homeland security research projects.

It is exciting to see such an audience of diverse interest that we have here today to address this important topic. This symposium has grown from a small gathering of faculty members on the campus of James Madison to a large collection of experts here at the National Academies. Today our goal is to connect broad policy efforts at the federal level to the important work being done across the country in local communities, at universities and especially the private sector.

I anticipate that this symposium will give us a new momentum to promote our efforts in IIIA and as partners. We hope that this symposium will promote future collaborations, and we will certainly welcome any tangible plans and proposals that you might have in this regard.

At this time I have another distinct honor. I regret that our President could not be here today. President Rose had a family emergency, and he sends his regrets. So I have the unique honor of introducing our keynote speaker for the morning. I have had the opportunity to get to know Congressman Dutch Ruppersberger over the last year, and to better understand the

person behind the post. There are few in our nation’s government who are as passionate when it comes to enhancing the quality of life for every American citizen.

Congressman Ruppersberger is serving his third term in the US House of Representatives, representing the citizens of Maryland’s Second District. The Congressman serves on the House Appropriations Committee and was also the first Democratic freshman ever to be appointed to the House Select Committee on Intelligence. This committee oversees the collection and analysis of intelligence information from around the world to ensure our national security and prevent potential crisis situations, especially as they relate to terrorist activities.

Congressman Ruppersberger is known as a consensus builder who works with members from both sides of the aisle and gets results for both Maryland and our nation. He has also demonstrated a unique ability in forming public-private partnerships, the theme of our conference. Operation Hero Miles is but one example of how this Congressman has brought together business and government to the benefit of the country and our fighting soldiers. If you are not familiar with this program, I hope that he will tell you a little bit about it. But in case he doesn’t, I feel compelled to say a few words about it. This program was created by Dutch in cooperation with close to a dozen United States airlines in October 2003. When started, the program allowed troops stationed in Iraq or Afghanistan to fly home on leave for free. It now gives family members of wounded service men and women free plane tickets to visit their loved ones recovering in military hospitals across the country. Operation Hero Miles gives U.S. citizens the opportunity to help our troops in a very direct way through donating their frequent-flyer miles to make a real difference in the lives of our soldiers and their families. The program is brilliant in its simplicity. Travelers donate their unused frequent flyer miles to the Fisher House Foundation. In fact, donations are currently being accepted from ten airlines. So if you would like, a tangible outcome of this conference could be some people donating miles.

Congressman Ruppersberger has organized new tabletop forums that have provided an informal communications vehicle -- I know he is going to talk to you about this as well -- between House Intelligence members and contractors and other entities to promote a genuine exchange of ideas and opportunities. Congressman Ruppersberger is someone who likes to get things done, and is not afraid to be innovative in his approach and to ensure progress. I think you will see that today. I am extremely pleased that the Congressman could take time from his busy work in the House to join us this morning. Please welcome Congressman C.A. Dutch Ruppersberger.

Remarks by Congressman C.A. Dutch Ruppersberger

HON. RUPPERSBERGER: Good morning, everyone. How are we doing this morning? Are we awake? I am going to talk about

some intelligence issues, some security issues, but as soon as I hear Hero Miles, I do want to highlight the program and give you some background how it came about.

When the troops were coming home for their R&R [rest and recreation] from Iraq and Afghanistan, they would come through the BWI (BWI Thurgood Marshall Airport), which I represent. In speaking with arriving service men and women, I would ask, "how are you doing? It is tough and I thank you for your service. Is there anything I can do?" Many replied, "I live in California or Arizona and I have got to pay a thousand dollars round trip to get home." I thought, here we are sending our troops to Iraq and Afghanistan, and now they have to pay their own way to come home. I tried to get money into the federal budget and it didn't work. So I used common sense. Based on my experience in local government for 17 years before coming to Congress, I went to the airlines said, "I have a very good program. It is a no-brainer for you, because it gives you good public relations. I call it Operation Hero Miles. With your help, I will go out and market the public and ask them to donate their frequent flyer miles so that the troops can come home." They agreed and I launched the program. I put together a website, went to about a hundred national shows. I spoke with Greta Van Susteren on two occasions. Within six months we had over five million frequent flyer miles donated. It didn't cost anybody anything.

After I had been in Congress for six months, I got a call from the House leadership. At that time the Republicans were in charge of the House and we had Republican and Democratic members saying, "Dutch, you can't do this anymore." I said, "What do you mean, I can't do it anymore?" They said, "You can't do this anymore because you are soliciting, and it is unethical." I said, "Wait a minute, I've only been here for six months and all I hear is what you can't do. I know I have the American military behind me and probably most people in this country. You might take my parking place away, you might do whatever you are going to do, but I am going ahead with this program."

Well, by the time I got on Greta van Susteren they couldn't stop it, and now we have actually made Hero Miles a law. Hero Miles has provided major benefit to our troops. But that is not what I came to talk to you about today.

Although President Rose couldn't be here, I'd like make a couple of comments about him. He is clearly a true leader who has transformed James Madison University. My daughter went to James Madison and lives in Harrisonburg today. In looking at President Rose's bio, I note that he was an assistant director of resident halls at JMU in 1975. That is more than a decade before the class of 2008 was born. There are only two reasons why you keep someone around that long: either he knows too much or because you can't imagine life without him. In this case I suspect it is both. So, President Rose, wherever you are, I hope everything is going okay.

I want to thank James Madison University for this homeland security symposium. Let's talk about the President James

Madison. He was the fourth President of the United States, and he saw some challenging times in his day. But I was always most impressed with Madison for his contributions to our Constitution. Whenever people referred to Madison as the Father of the Constitution, he protested. He said that the document was not the offspring of a single brain, but the work of many heads and many hands.

Today, likewise, the nation's intelligence business is the work of many heads and many hands. It is no longer just government heads and government hands. Instead, we rely heavily on partnerships among the government and the private sector including businesses, as well as academic institutions like James Madison University, the University of Maryland, University of Maryland Baltimore County and Towson University. You notice, I mentioned those other institutions because they are in my district. But I paid tuition at JMU.

Today I want to talk about two areas of national security that involve two very different relationships between government and the private sector. First I want to talk about intelligence satellites in the national security sector, where government is fundamentally in charge. We, the government, own the hardware in satellites. We define the projects, the parameters. We determine the mission and goals of new projects. Much of the work on satellites is done through contracts with the private sector. But the government decides what work gets done. Second, I would like to talk about some of the challenges facing our country in the realm of cyber security, an area where the government is not necessarily in charge. From a national security perspective, one of the hardest things about security in cyberspace is that the infrastructure is primarily privately owned and controlled, so improving cyber security requires strong partnerships among government agencies, private companies and academia.

It is important to realize that both cyber space and real space are critical to future national security. In the realm of real space we depend upon satellites, traditionally very expensive satellites. We are the strongest nation in the world because we control the skies. We have tremendously powerful satellites that give us a decisive advantage over our adversaries. Every corner of the intelligence community uses satellites to tell them what is happening on the ground, whether it is movement of troops or the construction of a nuclear reactor.

But our dominance in the skies is being threatened by China and Russia. Last year, China showed off to the world its ability to shoot down a satellite. This was a warning shot fired to show us that we can no longer count on American dominance in space. We need to design and build the next generation of intelligent satellites quickly, and they need to be able to meet the challenges of our country in the 21st century. We need our partners in the private sector to help us meet the challenge.

One of the lessons I have learned from my 22 years in government is that government doesn't always have the answers. Apologies up front to government people here. You are good people, but

you don't have all the answers. Oftentimes the private sector, whether it is for profit, business or a nonprofit organization or educational institution, possesses the best practices that we need to apply in building the satellites. Much of the expertise in designing and building satellites lies in the private sector. Government agencies simply can't offer the same pay and benefits as private companies can. We see many of our best and brightest engineers, mathematicians and rocket scientists move into private contracts as soon as they have gained the experience needed to make more money. I am grateful that we still have many of the smartest, most hardworking people in government.

I know that we have some of the topnotch people. I am chairman of the Technical Tactical Sub-Committee of the Intelligence Committee. This committee oversees for the National Security Agency [NSA], all of the NRO, and NGA. Our committee oversees policy and budget aspects for technical components. I am the first member of Congress to ever represent NSA. Since they are in my district, I spend a lot of time at NSA. We do have some of the most intelligent, smartest people in the world at NSA. I talk to numerous people and often ask, "Why have you decided to stay in the government? You can make so much more." These people answer, "It is not about money to us; it is about doing what is right for our country, and we love what we do." So we are very, very pleased that we have some great workers in not only NSA, but all over the government, especially in the intelligence arena.

These days, the government is facing some issues concerning satellites. Basically, in my opinion, the government should not be in the business of building satellites. In my role as Chairman of the Technical Tactical Committee, I have had the opportunity to interact many different businesses, subcontractors and also the government agencies that are working together to build our satellites. It is very hard work, and requires tremendous expertise. This is the business of companies like Lockheed Martin, Northrop Grumman, Boeing, Raytheon, General Dynamics and dozens of other companies and subcontractors.

As many of you know, we have some serious problems in many satellite projects. I can't tell you the names of those projects, some of them are classified – but we have had some serious failures in the last ten or fifteen years. Looking back at our history, when we first started to get into space, JFK said after the Russians came out with Sputnik that we are going to do what we need to do to protect our country. We, as Americans, responded with the expertise and ingenuity to place a man on the moon in 12 years. Now we are having problems getting a major satellite up in 12 years. This is unacceptable, and we have to change it.

Why are we having failures in our space industry? I think that one of the major reasons for failures is because we have not completed the research and development necessary before we start to manufacture. We need to make sure that we continue to put our resources and money into R&D, and uncover the

mistakes during the R&D phase before we get to the production phase. The costs of developing satellites are skyrocketing. Projects are years behind deadline. It is taking so long to build and deploy new satellites that we are now at risk of having an intelligence gap that makes us vulnerable to Russia and China. We cannot afford to continue to operate in a crisis mode.

Let me be clear. This is not the fault of any one company or government agency or Congressional committee. The problems we are seeing are caused by a lack of communication. For example, we have recently seen an acquisition effort being rushed as a result of a poorly defined RFI document [request for information]. The contractors were not asked the right questions. This problem had cascading effects. If the RFI didn't ask the right questions, how can the government release a good request for proposals (RFP)? This is just one recent example of how rushing the procurement process causes costs and delays for the agencies that would be using the satellites.

Consider this example. An RFP is released to meet an arbitrary deadline. The contractors respond, and ultimately a contract is issued. The government already knows there are contractual flaws that must be addressed and renegotiated at an increased cost and delay of schedules. All of you know that this is a problem. The government rushes to get a contract, thinking we can fix things later. The commercial sector does not do this. They can't afford to do this, or they would go out of business. If there are unknowns, they plan for them up front.

The problem is that requirements continue to be added throughout the life of a contract. A small, seemingly harmless requirement is added to a satellite development. Over time, additional requirements accumulate and, before you know it, the program is in serious trouble. In theory and practice, the project manager at the agency should be making all judgment calls about which additions or changes to the contract are necessary and worth the extra cost and schedule impact. Of course, a program manager must deal with many external influences. As another example, we just had to cancel a major satellite program. It was very sophisticated, but when you have three-star generals saying we need something else to go on this satellite, we have to change that system.

Outside of the agencies, Congress is responsible to conduct strong regular oversight of the satellite programs that I am describing. Far too often Congress must get involved because costs are spiraling out of control and newspaper stories are appearing about satellite systems that are years overdue and billions of dollars over cost. So agencies are responsible as well as Congress.

In my subcommittee I decided to replace the traditional Congressional hearings with what we call "tabletops." If you have watched a Congressional hearing, you know each member of Congress usually has five minutes to ask a question of usually the head of NRO, the head of CIA, or whomever. This approach has been problematic for sophisticated technical programs. In

a program involving satellites or cyber networks or whatever we deal with, it is difficult to get into the meat of any issue with a five-minute question. By the time you get an answer your allocated inquiry window is over.

So I decided to try a different type of strategy in the Intelligence Committee involving tabletops. In this new venue, I have the major contractors and representatives from, say the NRO [National Reconnaissance Organization], come into our hearing room in the Capitol. Our committee meets in the top of the Capitol. For four or five hours we sit and discuss issues about our satellite program, using the satellite as an example. I start out every hearing by stating that, after the Russians launched Sputnik, we responded by having a man on the moon in 12 years – we have to get back to where we were. Next we look at our failures and our successes. Many times we only look at failures; but we also need to look at successes. Then we discuss where are we now, where are we going to be in the future, what systems we have in place, and how much is it going to cost.

And believe me, cost is a major issue – a very serious issue right now. Right now, in Iraq, we are spending between \$10 to \$12 billion a month. That is a billion. Because of that there are a lot of areas and programs that are being cut that should not be cut. In my opinion, from a national security point of view, our country is consequently at more severe risk. If Russia or China can dominate the skies, as we do today, and they are getting very close; I believe that is more serious than terrorism and the things that we do to counter terrorism. The tabletops have been very successful. We have had about nine tabletops. If we have an issue with complex technical systems, we use tabletops.

I can say this because it is not classified – it has been in the paper. We had some energy issues at NSA. Those of you who work at NSA know that there is a lot that we do with the equipment and how we collect and analyze information. Yet if you have energy issues, you are going to be in deep trouble. We successfully worked through this problem. We brought in the people from NSA. We brought in experts, we talked about funding, and now I am happy to say that issue has been resolved. But we solved it using the tabletop process.

Because of the success of the tabletop approach with House Intelligence, Senate Intelligence has also, just recently, started that process. I think that bodes very well for the nation, but it also is all about partnerships, the subject of this symposium – partnership between business and government. We have tabletops based on such partnerships. We bring in all the players. When the deliberations are finished, we write a report, make recommendations and move forward.

I now want to get into the other issue I want to address this morning – cyber security. We have talked about satellites and their current problems. Failure is not an option when it comes to the satellites because of what is at stake. But cyber security is a whole different issue. The problems I just mentioned

regarding our satellite acquisition process are easy compared to the challenges posed by cyber security. Independent of whether the government owns a satellite or just leases services from a commercial satellite company, the government can define specifications and expect the performance it needs from the asset. But the government does not own the Internet. It is impossible to control this realm of communication. So how do we secure not only the Internet, but everything connected to it?

Our critical infrastructure like the power grid, our financial systems and so on are all on decentralized networks owned and controlled by everyone and no one. But their security is an essential element of our national security. Just imagine the Bank of America network suddenly coming under a successful attack.

By the way, we are under attack every day. It is not classified. We know that we are under attack at the Pentagon. We have that under control, but we are continually being attacked – not only by other governments, but by independent hackers. We are very much concerned about terrorist exploitation of such attacks.

Bank of America has 59 million customers in 150 countries. If there were a wide-scale cyber security attack, it is possible that every one of them would suddenly be unable to access his or her account. You take your debit card to the grocery store and are unable to buy food because the bank's network is down. ATMs can't dispense cash. Credit cards are useless. Even the tellers at bank branches would be powerless to help, because they rely on the same network the rest of us do.

What would happen? First, we would see a bank run like never before in this country if Bank of America was attacked. Even other banks unrelated to the Bank of America would have customers lining up at the door to withdraw money that no longer seemed safe. Even if Citibank and other banks were still up, the panic would likely spread to throughout the consumer banking community. The financial markets are also likely to panic with dire consequences to the entire economy. How can one of the largest financial institutions in the world survive a crisis like this? And what are the consequences for every corporation that has accounts within that bank? Even if the network was only down for a day, the ramifications would be throughout our economy with potential catastrophic consequences.

What I just said seems pretty farfetched, but it is not. Surely someone can't just take down the network capabilities of an entire corporation. We can't say for sure at this time. I believe that another government could do this. What we do know is that the Russian government knows how to take down the network capabilities of an entire country. In April and May of last year, Estonia websites were subject to rolling cyber attacks. These attacks incapacitated the websites of the Estonian national government, communication firms, political parties, three of the country's main news organizations and two of its largest banks. The Estonian government believes that these attacks were launched in cooperation with or on the orders of

the Russian government in retaliation for Estonia removing a Soviet war memorial in the capital city of Tallinn. Of course, Russia denies any complicity. But several of these computers involved in the attacks were traced back to Russian government agencies. Regardless, these attacks show that it is all too easy to use basic Internet hacking techniques to wreak havoc with a nation's information infrastructure. Estonia is a small country of 1.4 million people. That is about the size of Philadelphia. The United States obviously has far greater resources and expertise to prevent this sort of attack. We have the best network security experts in the world. DISA [the Defense Information Systems Agency] is moving to Ft. Meade, in my district, in 2009. This agency is responsible for the network security of our defense and intelligence communities around the world, and they do a great job.

The problem is that cyber attackers, whether part of a foreign government, a terrorist organization, or a group of individuals who wish harm on our country, don't need to exploit vulnerabilities in our government's network. Based on the Bank of America hypothetical attack, taking down a product company would do real damage to our country. Whether it is banking or communications or energy, much of our country's most critical infrastructure is in the hands of private companies.

But even if attackers could get to a bank or an airline company, at least our national security systems are safe, right? However, the Internet is a network, and a network is only as secure as its weakest point. Our national security networks are connected to the outside world. It might not seem so critical for the University of Maryland School of Dentistry to have topnotch state of the art network security. Why would someone want to get into their network unless they are into dentistry? But the School of Dentistry is connected to the larger University of Maryland network, and the University of Maryland works with NSA. (By the way, I went to the University of Maryland, so that is why I am using that as an example.) So a hacker that gains access to the dental school can gain access to the whole university network, and they can use that to come in the back door of NSA's system. The ability of hackers, from terrorist organizations to unfriendly nations to disrupt our networks has fundamentally altered the strategic landscape. The Internet was not developed as a secure network, yet today much of our sensitive business goes out over the Internet.

So what do we do about this? We need a public-private partnership to secure every network in the United States. The hard part is that, unlike satellites, the government can't unilaterally decide how the Internet should be organized or secured and hire someone to do it. Ninety-eight percent of Internet traffic runs on private networks. If we are going to protect our critical infrastructure, we must engage the private sector in the cyber security initiative. Every company that has a server sitting in its back room has to be a part of the solution. While the largest companies in the U.S. – Bank of America, AT&T, Constellation Energy and Comcast – have the resources and experts to develop

state of the art security systems, smaller local companies do not. We need to grow the network security workforce so that small and medium sized companies and institutions have access to the same expertise as the huge multinational corporations. James Madison University was ahead of this curve. In 1997 the university established its information security program. Today the program has graduated nearly 200 students who have gone on to take senior roles in helping government and private sectors secure their critical infrastructure. These are critical skills at critical times. By offering courses in advanced network security and computer forensics, JMU and its graduates are contributing to our national security.

To summarize, government and industry have worked together to make our nation more secure for more than a century. We have brand-new challenges facing us in cyber security, and our traditional dominance in the world of satellites and overhead architecture is threatened by other nations. We cannot take our eye off the ball, especially with regard to China and Russia. But I have every confidence that we, as Americans, by working together, by educating our students, will meet these challenges and keep our country the strongest in the world.

By the way, is Mike Delaney here? Mike Delaney is the chief of staff for our Intelligence Committee. His daughter attends James Madison, so I invited him to be here. Bob Minehart is my staff director for the Committee on Technical Tactics, and he is out here. He is also an engineer and has worked at NSA and CIA. Now he is on our committee. So wherever you are, Bob, thanks for being here.

Thank you for having me here today. I am going to open up for questions.

Discussion with the Audience

DR. O'NEILL: Don O'Neill, Center for National Software Studies. Public-private partnerships have been encouraged and are very good in certain areas. Sometimes they evolve or devolve into go-along/get-along cultures. The real issues don't get raised across different stovepipes. I am interested in your thoughts on having some market driven incentives that would encourage people in stovepipes to engage with people in other stovepipes, things like self-help remedies analogous to your getting the soldiers some free air travel. That is a good self-help remedy. But I am thinking of self-help remedies that would have indemnification for a reasonable range of side effects that might occur. I am thinking of insurance mechanisms, tax policy, and legislative investment.

HON. RUPPERSBERGER: Let me stop you for a second. Are you talking about within the government structure, or with the partnership between government and the contracts that we gave as incentives? Is that where you are going?

DR. O'NEILL: Yes. I'm concerned about public-private partnerships that depend upon people of good will working

together that sometimes they do almost too much because they get into go-along/get-along situations. By this I mean that they don't really drive the issue across stovepipes because they know they are goring someone else's ox. I'd like to see public policy incentives that would encourage the different stovepipe operations.

HON. RUPPERSBERGER: Give me an example of a public policy incentive.

DR. O'NEILL: A public policy?

HON. RUPPERSBERGER: Yes, if you were the boss, wherever you are, what would you put in as that incentive?

DR. O'NEILL: I would give tax credits to the financial industry if they would coordinate their recovery time objectives with the electrical and the telecommunications infrastructures so that when they say they can be up and running in four hours they will have the supporting infrastructure to open the next day. They could really do that because they have made provision for crisis management in a way to make it happen – not in a risk management mode where they make a list and study the problem as opposed to taking action.

HON. RUPPERSBERGER: First thing, I think incentives are great idea. Let's talk first about the basics of management. What makes a good manager? First, every good manager will hire good people. That manager will give those people the resources to do the job. That manager will motivate his or her people to do the job, but the manager must hold them accountable for performance. So you must talk to your front line. In the area of sales is a good example of the value of incentives. Believe me, if you are a salesperson you want to be on a commission, not just a straight salary, because you get incentives to go further.

Stovepipes are a problem in infrastructure assurance, and one that we could discuss for hours. It is difficult because it is so technical. The objective is to have solutions that are on time and on budget. If you are on time and on budget maybe you have a bonus program for your front line and your employees to give them the incentives, as long as you do it in an equitable way. A major problem is that government gets clogged. It can happen in business, too. It can happen in a college administration. You have people that have been in the same job forever and are not thinking out of the box and not moving forward in their ultimate mission. I think you are right in saying the same thing can happen with private-public partnerships

We just talked about satellites. We can no longer afford have satellite programs cancelled after having invested billions of dollars. I think that the problem is accountability. That is poor management at the top when you have those failures. We need to analyze and improve our accountability processes. I have emphasized the importance of research and development. During the R&D phase, it is not straightforward to provide incentives based on final satellite design and operational capabilities. I

agree with your points from a management perspective. We have to break down the stovepipes, no question. That is why China and Russia are going a lot better. They have learned from us and they have tried to avoid problems we've had and take their approach to another level.

DR. KLAU: Good morning. Stephen Klau, Center for Strategic International Studies. When Sputnik was launched into orbit, and at the time the Soviet seemed to be ahead of us in engineering and space, there were incentive programs for people to go into college and learn the sciences and engineering. Now we seem to be in a similar situation, where other nations seem to be exceeding us in similar areas in technology. Is there a possibility that we could reintroduce some of these incentive programs to increase our education in colleges in engineering?

HON. RUPPERSBERGER: I am concerned about this and will tell you what I am doing. We are not having our young minds going into the areas of space and technology as much as we should. The only way we are going to do that is to work with our universities to make sure we attract the best and the brightest minds into science and technology.

China is an example. I was over there about eight months ago. The China takes their people with the highest abilities in math, rocket science and engineering and, because it is a Communist country, they force them into technical degree programs and work in their space industry. Also, China has learned a lot from our country because we have graduated a lot of Chinese students. In the past they would stay and become Americans. Now they are going back to China. Just last year, the United States graduated 60,000 engineers. That seems pretty good for the United States, but China last year graduated 600,000. The good news is that our curriculum is still superior to theirs. But, they are getting closer.

What am I doing as a member of Congress? You know how long it takes to get things done in Capitol Hill. When I came back from China, I met with the NSA board. Google and Microsoft representatives sit on their board. I asked General Alexander, the head of NSA, to introduce me to some of his board people. My idea is to come up with a STEM [Science, Technology, Engineering and Math] program starting in middle school. I want us to identify students with a technical aptitude in middle school and then high school, and start a regional program in the Baltimore area around NSA to include people from inner city. The program would include aptitude testing. We will be working with our state school superintendents.

I met with Bill Gates on this issue. Microsoft is very interested in helping us, along with other major companies. One of the big challenges we are talking about is getting the right teachers. When you go into a state education program, sometimes you have to worry about teachers unions and issues like that. Because we want to hire the best teachers for, say \$100,000 a

year, and Microsoft is going to help pay for it, we will need to be very selective. We need the best since we are competing with China and Russia.

We are in the process now of moving forward with that program. Once we have the program in place here, we are hoping that it will serve as a pilot program for other areas. The NSA focus is important. We want the kids that are going into the program to go to NSA; we want them to start feeling what it is like to be an American, to be working for your country, to be motivated by patriotism. Just like someone who has aptitude in art is encouraged to attend art school or drama school, we want to encourage those with technical aptitude to pursue the best related education. We have to do it.

You started with Sputnik. We responded by pursuing the research and development necessary to send a man to the moon. This effort was a major factor in why we are the most powerful country right now. During the moon program, we didn't look to dominate in other areas but many unforeseen strategic and technological benefits resulted. As it turned out it was a good thing, because if not, China could be more dominant than we are, and they are getting very close. They knocked out their own satellite to test their capability, but also to send us a message that they can do it. By the way, to remove a satellite that was out of control, we have also successfully demonstrated our capability.

MR. RICE: John Rice. I am with the Department of the Navy. Listening to your comments about the satellite acquisition programs, the situation is very similar to problems the Navy has with the acquisition of ships and other services' acquisition of weapons systems. The government can't afford the expertise that we need. People leave and work for industry.

Then we talk about partnership. Partnerships require an equal level playing field. What are we going to do so that the government can attract and hold onto the graduates that they need so that we can at least ask the right questions when we put out the requirements, the RFI, and the RFP documents? We need the expertise to determine and evaluate the requirements in a credible way, rather than just writing checks.

HON. RUPPERSBERGER: First thing, writing the checks is part of the problem. We are the client. When we buy something, we had better make sure that it is right. One of the things that we are looking at right now, and there is a lot of controversy in this issue, are the comparative risks/benefits of our current process of satellite acquisition under complex contracts with the big aerospace companies, versus leasing commercial satellites for the functions of interest. The commercial satellite industry has to get it right. They do their research and development ahead of time because, if they don't do it right and they have a failure, they can go out of business. So that competition between commercial satellites and the way the government builds satellites now is very, very important. I have raised this as an issue, as committee chairman, and working very closely with the DNI, Director of National Intelligence and Don Kerr, who was head of NRO and is

now Deputy Director of the DNI. I have also been working with General Clapper, former director of DIA and General Cartwright, who is also working in this field. We are all looking at the issue of commercial satellites.

Because Europe didn't have the money that we had and didn't put the money in defense, they have relied on the commercial sector and now they are ahead of us. If we don't watch ourselves, Russia and other countries may move ahead. So we need to revitalize our American ingenuity.

I have discussed this issue with the big companies that I mentioned during my talk. The idea is to rent instead of buy, but the government would still have flexibility in specifications. Leasing also provides access to multiple satellites. This is an option that we need to carefully consider.

Sometimes we get lethargic. Things are done the same way by people who have been around a long time. We are all guilty of this. We need to look out of the box, to see what is going on in the rest of the world. Friedman wrote the book, The World Is Flat. We can't be thinking that we are so big and powerful that other people are not going ahead of us. That is the debate that is going on right now concerning what we are going to do in this field.

MR. PARDY: Andy Pardy with DRA Enterprises, formerly with DHS. Is Congress more concerned about addressing the international component of cyber risk and cyber preparedness than the executive branch appears to be?

HON. RUPPERSBERGER: I know I am personally because of where I sit. I am very concerned. We are under cyber attack on a continual basis. There are many issues of civil liberties that are out there. I think government will be able to handle this issue with NSA. They have major efforts to address technical issues related to cyber risk. My concern is for the country and the business community. Roughly 80% of the Internet infrastructure resides in the business community in the United States. I'm not sure if that is the exact percentage, but I think 80% is close.

What really concerns me about that cyber issue is that all businesses must understand that they will need to allocate resources and hire experts to make sure that their systems are secure. It relates to the "weakest link" problem I alluded to. Bank of America might have a small branch somewhere in North Dakota. It could be a very small community bank that is tied into Bank of America system. The Chinese could get into the main network through that small bank. It's a real problem that must be addressed.

So we must let the country know. Security must become a marketing consideration. Civil liberty is important to all of us. There are those who say that the government should not be involved at all in the cyber security issue because of civil liberties. Believe me, the more the government is involved and the business community is involved to set up a defense mechanism

for cyber attacks, the more security you will have. I say to people about security, "We already know your social security number, Medicaid, Medicare," so the government is, of necessity, already involved in cyber protection. This is an extremely high priority endeavor. We didn't foresee its seriousness as soon as we should have. We are looking at it now. I know that General McConnell, our ODNI, sees this as a very high priority. We don't know who the next President is going to be right now. I haven't heard. My specialty is intelligence and the things we are talking about here today. I'm not sure whether it will either be McCain or Obama, but in either case, I don't want somebody from the new administration to come in and say, "We can cut billions of dollars by not proceeding with a cyber program."

Again, terrorism gets a lot of attention. But, in my opinion, our biggest threats to our national security are related to the skies and the cyber. I know that members of my committee feel this way. I'm not sure where the new President will be. I know we have a huge public educational process ahead of us to let people know that they will need to pay an extra dollar or two so that whatever you do can be secure. Banking, energy, the power grid, all these things must improve their cyber security.

In closing, I'm happy to be here today. I hope I have been able to inform you a little bit about where we are and what we are doing. I thank you all for what you are doing in the field that you are in, whether you are in government, academia or the private sector. The most important thing is teamwork, coming together. If we can do that and keep our American ingenuity, I think we are going to be successful. But we have got a lot of hard work to do.

Thank you.

Introductions by Steve Knickrehm

MR. KNICKREHM: Thank you very much, Congressman, for those enlightening and inspiring words. Also, thank you very much for paying your tuition. It goes to pay most of my salary and the salaries of a lot of other people in this room. We greatly appreciate that.

Following up on the Congressman's themes, he presented ideas that deal directly with our program today. The first is best practices. We have put together three panels in which we include examples of best practices. We hope that you can learn from these examples. That is the intent.

Congressman Ruppertsberger also mentioned learning from our successes and our failures. The panels have been put together to not only tell you what the public-private partnerships are, how they operate, and what made them successful, but if they had difficulties in getting to that level of success, to inform us of them as well.

The structure of the agenda is as follows. We will start with our panel on local public-private partnerships. We will move on after

the break to our panel on regional partnerships. Then, after lunch, we'll address national partnerships. You will get an idea to successful examples of public-private partnerships on three different scales. This structure was originally proposed by Lynda Stanley. Thank you Lynda. Your theme has worked well.

Our first panel participants are experts have established an exemplary local public-private partnership and come to us from Long Island, Nassau County. The program indicates that Inspector Matt Simeone will be the moderator. Inspector Simeone was not able to be here today due to illness. Indicative of how well-esteemed he is in the Nassau County Police Department; his boss is here to take his place. So I am going to introduce his boss, Chief Tully; and he will introduce his panel.

Assistant Chief Tully is with the Nassau County Police Department. He is a 35-year veteran in the Nassau County Police Department. He is currently the commanding officer of the Homeland Security and Counterterrorism Bureau there. "SPIN," the public-private partnership that is the subject of the panel, is within his bureau. Chief Tully has a B.A. from Hofstra University and holds a master of professional studies in criminal justice from Long Island University's C.W. Post Center. He is an adjunct professor at Nassau County Community College.

Panel One: Nassau County Security/Police Information Network

CHIEF TULLY: Thank you very much, professor. I appreciate the invitation to be here. I would like to thank the James Madison University and National Academies of Science for this opportunity. I definitely feel like a pinch hitter, coming up from a farm league to the major leagues in the ninth inning of a big game. That is how my friend and colleague Detective Sergeant Bill Leahy described it today.

So it made me a little bit nervous when I came into this hall. I had learned last night that this is where President Kennedy announced his space initiatives, referred to by the Congressman. When I look around the room, and I know who is in the room, following the Provost and the Vice Provost and the Congressman, it definitely is a very impressive group that we you are addressing. We are very happy for this opportunity.

I know what the Congressman was talking about concerning cyber terrorism. It is a very large scale problem. What we are here to do is cast the subject in terms of public-private partnerships. This is where the rubber meets the road at the local level. I will first read a very brief description of the Nassau County Security Police Information Network, which we refer to as SPIN. SPIN is a dynamic, multidimensional crime prevention partnership between the Nassau County Police Department and the private sector that seeks to increase public safety through the sharing of important and timely information. This program is designed to promote homeland security initiatives and business continuity as well as foster the exchange of information that is critical to the success of protecting Nassau County residents and businesses.

The goals of SPIN are to share information, identify and discuss crime trends and solutions, and work together toward the common goal of protecting persons and assets.

SPIN enables the police department, or any other county agency, to send out information to the general distribution group or to a specific sector. In addition, SPIN connects local, state and federal law enforcement agencies operating in Nassau County, as well as public transportation and other federal agencies. As a result, SPIN's multi-tiered approach allows messages to be tailored for law enforcement, vetted security directors, chambers of commerce or civic organizations.

This is the accepted, very general description of SPIN. But what does it really mean? Before I introduce the panelists, to get to the essence, we will give you some personal observations on the benefits SPIN. We will start with Bill Leahy.

SGT. BILL LEAHY: As a detective assigned to a squad investigating bank robberies at one point, the ability to disseminate a picture that is downloaded from the scene of the crime and disseminated instantly through cyberspace to 365,000 participants is a very good tool for me to have at my disposal.

MS. OKSANA FARBER: When this question was posed to us last night, initially we were asked, "Imagine what it would be like without SPIN." As a business person, imagine running your business, your school, your organization with the confidence that your local police department is there to do a lot more than just protect and serve after an event. Imagine your local police department as a business continuity partner, someone who is there to provide you with the daily, real-time information that can make you less vulnerable and help you avoid becoming a victim.

MR. DOYLE: Thank you, Oksana. Imagine being responsible for the security of a power plant, and noticing an individual take pictures outside your facility. Now, is that a college student doing a project or is it pre-operational surveillance? Imagine having a centralized resource within the Nassau County Police Department that could take that information and assign it to the proper squad. In addition, imagine being responsible for a facility and being notified immediately of police activity that is headed your way. Imagine being able to take the steps needed to protect your facility if that activity ends up on your campus.

CHIEF TULLY: I will now introduce the panelists.

Immediately to my left is Detective Sergeant Bill Leahy, William Leahy, of the Nassau County Police Department. He has 23 years in policing. He had spent five years with the New York City Police Department, followed by this last 18 years with Nassau County. He is assigned with me to the Homeland Security and Counterterrorism Bureau, but his responsibilities include the day-to-day operation of SPIN. During his distinguished career, Sergeant Leahy has been recognized within his agency as both a creative, problem-oriented police officer and as a talented

detective. His work has been recognized by the International Association of Chiefs of Police as a semifinalist for the esteemed Web CV Award, and by both the National League of Cities, and Police Executive Research Forum with awards for excellence in problem-oriented policing. He also is a graduate of the FBI National Academy.

Oksana Farber is Vice President of Operations for Hiram Cohen and Son, an insurance and risk management organization. She has over 25 years executive leadership experience and is a profitability-oriented business strategist with expertise in human resources and operations facilities management. As a chief security officer, Ms. Farber became an active member of ASIS International [American Society of Industrial Security], where she formerly served as New York City Chapter Secretary, and currently serves as Vice Chair of the Law Enforcement Liaison Council, a national body whose mission is to build partnerships between private security and law enforcement. Ms. Farber has written articles for several security publications including articles on building relationships, developing information sharing partnerships post-9/11, and developing cooperative relationships between human resource and security officers.

Mario J. Doyle serves as the Vice President with Building Star Security Corporation, one of the leading providers of security services in the New York-New Jersey metropolitan area. He has held several senior management positions with national and regional security firms, and has a broad range of security management experience, including corporate operations and compliance, personnel training and standards and quality assurance. In addition to being an established business executive, Mr. Doyle has been active in the law enforcement community for over a decade, and is a founding member and co-chairman of the Nassau County Law Enforcement Exploring Advisory Board. He also is a director for the Nassau County Police Reserves. He is a licensed New York State private investigator and has earned certified protection professional certification from ASIS International, for whom Mr. Doyle serves as the regional vice president of the New York area.

I am pleased to have such distinguished panelists. During this session, I will ask them to cover the background of SPIN, how it started, how the network was built, provide some examples of real SPIN experiences, and also take a look at the future of SPIN. Before we start with SPIN, we must say a few words about Nassau County. I'm sure we have some Long Islanders and former Long Islanders in the audience. Bill, it would be helpful to give us a brief description of Nassau County.

SGT. LEAHY: Nassau County is one of the four counties on Long Island. We border New York City on our west side. We have roughly 1.3 million people in our county and are bordered by water on both north and south. We have 4,000 members in our police department, 2700 of whom are sworn. Based on Forbes and Money magazine articles, we have consistently been considered one of the safest counties in the U.S., among those with the lowest crime rates.

CHIEF TULLY: Thanks, Bill. You were there in the beginning, Bill. How did SPIN start?

SGT. LEAHY: SPIN was really an outgrowth of 9/11. As the subsequent, follow-up reports began to emerge about the problems with information sharing and intelligence gaps and stovepipes that have been mentioned earlier, we began to realize that we were subject to the same problems. Studies indicated that approximately 85 percent of critical infrastructure is in the private sector hands. In most cases, the private sector controls the operation and the location of target infrastructure, and we control the information. We recognized the need to put those two together. We wanted to start talking, not under the guise of, "I'll tell you what you need to know when I think you need to know it and when I want you to know it," but rather in terms of establishing a true, open partnership.

Our then-Commissioner James Lawrence, a former chief in New York City, attended an FBI Law Enforcement Executive Institute conference on public-private sector partnerships. He was intrigued to learn about the lack of partnerships between law enforcement and the private sector. He came back to Nassau County and began to research partnership possibilities. At the same time, a retired sergeant, who formerly worked in New York City under James Lawrence, was working as a continuity planner for Citicorp. He approached the Commissioner and said, "I think we need to begin a dialogue." In the same time frame, Oksana Farber, head of the Long Island ASIS International law enforcement chapter, penned a letter to the Commissioner stating that it was time for our organizations to form a relationship.

CHIEF TULLY: Oksana, you were with ASIS International at the time and I think you were the law enforcement liaison. Could you tell us a little bit about ASIS International and the role that you and ASIS had in starting SPIN?

MS. FARBER: I'll answer both questions, one at a time.

It is extremely important that we inform you about ASIS International, because the type of training and networking that we were able to get through membership in that organization was essential to creating and developing SPIN. We also brought some print literature. We urge you to please take it with you. It explains everything that you may want or need to know about ASIS International. If you gave us an hour, we could talk about ASIS International and still not tell you everything, so we decided just to highlight four or five points and how they helped us to develop SPIN.

ASIS is a global security organization of public enforcement and other public agency members, like the FBI, CIA, private security directors, chief security officers, and corporate security officers. Four years ago, the name was changed to ASIS International because we have been a global organization for more than five or six years now. Most members participate at the local chapter level. The largest chapters in the world are in Washington, D.C., New York City and one in the United Kingdom. ASIS International

is the standard for creating practice guidelines for the security industry by certifying CPPs, PCIs and PSPs. The CPP is a certified protection professional, PCI is a professional certified investigator and a PSP is a physical security professional. ASIS International collaborates with the Wharton School at the University of Pennsylvania by offering security executive leadership training. ASIS International's staff is also supported by a highly skilled lobbyist who helps to promote and support legislation on issues such as discrimination, drug testing, border security, intellectual property, identification theft, and gun control. The organization is also serviced by 30 different volunteer leadership councils from related industries. The Law Enforcement Liaison Council is the council that I am affiliated with. We promote, develop and help to maintain effective relationships based on rapport and reciprocity between the public sector and the private sector. Lastly, Security Management magazine is published by ASIS International. It is the most reliable source for security products, security organizations, and emerging trends. The handouts include a copy of an article about SPIN published in June 2006. That is a rather lengthy answer to the first question.

Now, about my involvement and the role that I play in SPIN, to help you understand, let me explain to briefly about what started out as a professional frustration and then became a personal passion. My involvement with ASIS International and the police department began when, as an HR director, I was thrust into the world of security when my warehouse employees reported to me that we were experiencing workplace violence, internal corruption, identification theft, IT manipulation, physical security tampering and aggressive thefts. My organization was also was subjected to grand larceny.

In assuming the additional role of the corporate security officer, I found that I was woefully unqualified. My quest to learn about security led to my discovering ASIS International. I attended classes, seminars and training every month for about a year and finally got up to speed. I learned quickly about cyber security, physical security systems, investigation and interrogation and diversity training. The training was invaluable as I was responsible for developing and implementing security policies and procedures for my employees. However, during the security cleanup of our warehouse I discovered the police department in my county did not talk to the police department in the neighboring county. I became extremely frustrated when we had no recourse except to hire private security to help us establish business continuity and recovery. I also had to hire undercover operatives and install and operate surveillance.

Prior to September 11, 2001, a similar lack of communication and cooperation existed with many other agencies - not just local ones. To make a long story short, I was surprised when the Suffolk County district attorney approached me and about establishing a network to share information between the private sector and the police department. He asked me to reach out to chief security officers in the private sector - particularly those who represented critical infrastructure in huge organizations like Computer

Associates and Shearson-Lehman Brothers. Unfortunately, that program fell apart. Nevertheless these organizations were willing to share our resulting white paper plan with the Nassau County government. The police commissioner took it ran with it. In six months time the county worked miracles.

CHIEF TULLY: Sergeant Leahy was right in the middle of this and assigned Inspector Simeone and yourself to do something about it. Sergeant, how did it get started? What happened next?

SGT. LEAHY: The first thing we did was to reach out and do a little research. We discovered that there wasn't a lot of information on public-private sector partnerships. What was available was very narrow in focus, sector-specific information. We were looking for a broad approach – all crimes, all hazards, and all threats – to improving our system. We read the Suffolk white paper. IACP had put out a book on operation cooperation. We were also getting tidbits from the newly released 9/11 Commission report concerning the lapses in information sharing.

Our first initiative was to organize two focus groups. The first focus group was within the police department. We took supervisors, detectives and specialized units and asked them what was important to them, what information they would like to disseminate, and what information they needed from the private sector. We took that information, categorized it, and figured out what was important to us and how information sharing would work.

We then formed the second focus group using the ASIS organization mailing list. This focus group involved people from different disciplines who were tasked to address what they expected from the police department including what they would like to see in the way of information, what were their frustrations, and how the police department should approach the problem. Using that information and Oksana's input, along with the white papers, we began a review of our program.

CHIEF TULLY: Oksana, at this point what did you see taking place?

MS. FARBER: We saw walls of silence. We were not sure how to chip away at these barriers. It is understandable, because within a structured environment like the police department, the information equates to power. Asking these gentlemen in the police department to re-evaluate what truly was law enforcement sensitive and what was not turned out to be a good beginning point. In the end, we perceived the silence to be a much bigger obstacle than it actually was. We discovered that once we brought together the private sector with the police department, the police department was shocked, delighted and surprised to interact with the business community. The private sector had been clamoring for a long time to actualize such an information sharing relationship.

CHIEF TULLY: At this point, you had developed the focus groups. How did you build the network?

SGT. LEAHY: We initially reviewed some related programs. New York City Police Department had a very successful program for a long time called the APPL program - the Area Police-Private Security Liaison Group. That was a great starting point for us. The one downfall that we saw, based on the focus groups, was it was overtaxing the available data sharing technology. Available software supported, "we will tell you the information, we don't expect any replies or we will give you the information but we will keep it short and brief." Still, the APPL was a great starting point because the network was already built. We looked at some off-the-shelf, custom applications. We gathered information from some vendors. Cost became a very big issue for us.

The police department already had Microsoft Outlook. Thus, Microsoft Outlook came at a perfect price. We were familiar with it and it had also been accepted in the business community. The challenges included how to staff the data sharing process and what information we were going to include.

Using DHS' critical infrastructure sector strategy documents, we adopted their sector classifications to start the group. We were able to get two police officers from patrol, Sue Pichiano and Jesse Atchison, to handle the day-to-day coordination while I provided operational oversight and figured out what kind of information we wanted to send out. That was the genesis of SPIN.

CHIEF TULLY: Mario, how did you get involved with SPIN?

MR. DOYLE: I was the security director responsible for one thousand security/public safety personnel on Long Island. I received a letter from Commissioner Lawrence at the time, asking me to join the SPIN network and inviting me to the inaugural meeting. Attached to that letter was a SPIN application asking for personal information. It specified that the membership of SPIN would be vetted through the police department. Frankly, I was amazed.

Another feature that impressed me was that the police department was now looking to build a network that shared all information – all crimes, all threats, all hazards. Think about that. It is revolutionary for a police department to release such broad information to private industry and inform us that they truly want to establish a long-term partnership.

We vetted the security directors and the personnel that were going to be members of SPIN to make sure that our information sharing was acceptable and the process well thought out. This process made provision for SPIN to incorporate two-way communication. I was familiar with NYPD's area police-private liaison program. As Bill mentioned, it was a good program but it included only one-way information flow.

CHIEF TULLY: Thanks, Mario. Why did the private sector need the information you referred to? What is the value of that content and information to the private sector?

MR. DOYLE: From a values standpoint, it was a centralized resource that the Nassau County Police Department was creating. I was in the private sector. Our relationships, if they existed, were

with the local precincts. Relationship to the police departments occurred only if the private organization had a staff member that was either retired from the police department or that had built up a relationship with the local precinct. But imagine being the individual business owner or the individual business in Nassau County that didn't have a retired law enforcement officer on staff or a relationship with the precinct. How would you get started?

When the Nassau County Police Department developed SPIN, I looked at its value to the public sector in providing them a direct, centralized resource to coordinate their law enforcement needs through the police department.

CHIEF TULLY: Oksana, did you want to add anything to that?

MS. FARBER: SPIN is something that the private sector had been hoping and wishing for, especially since most of us who conduct business out on Long Island also conduct business in Manhattan. We also had the APPL network, which eventually became NYPD Shield, and we were wondering when something was going to happen out on the island. We were pleased that we didn't have to wonder long. The two-way e-mail communications that SPIN established is a wonderful idea. It is really the only way to do it.

CHIEF TULLY: Thanks, Oksana. We have been talking about private security. Bill, who else is in SPIN?

SGT. LEAHY: We originally started out with 60 security directors, and then we began to realize that the group needed to grow. There are a lot more applications beside the critical infrastructure. Specifically, I mean any local business that may be the target of crime, the target of vandalism, the target of harassment, but more important than that, serve as extra eyes and ears on the street for us. We began to realize that the members of SPIN act as force multipliers for us. Every security director that gets a message sends that out to his staff or his security staff, and now we have extra eyes and ears on the street, educated, assisting us in our mission of protecting the folks.

Looking at the PowerPoint chart, you will see that we act as the center and we are a virtual public-private sector partnership. Through the different layers, we have our vetted critical infrastructure groups. Our network expands out from these. But government also has the same clients, the same missions. We overlap jurisdictions. One of the things that we look to do is help other government organizations. There may come a time when the department of health needs to send information out, including pandemic information, influenza information, and seasonal spraying information. We can pre-empt having to handle hundreds of calls about the low flying airplane dropping aerosol late at night, by educating our groups through the SPIN network system.

So, we can use the Office of Emergency Management as a vehicle to aid information dissemination from our department of health or our court system. We have expanded that even more into

a regionalized group working with New York City's Shield and Suffolk County. If you are doing business in Nassau, it is great if you are located in Nassau. But if you are located in Suffolk and doing business in Nassau, you should also have an opportunity to receive the information. Transportation businesses are a case in point. They have become an important force multiplier for us since they span multiple jurisdictions.

After the first year, we began to realize that we had left out an entire sector. We were looking at security professionals. We were looking at people in business who we vet and trust. But there was a large remaining group that we needed to incorporate, another layer of force multipliers – the civic associations. They don't need business continuity information, but we made arrangements for online information and training to cultivate an educated, smart and aware group from chambers of commerce, Kiwanis clubs, neighborhood watch groups, civic associations, and other social organizations. We teach them how to be better witnesses online. If you are familiar with James Wilson and the broken windows theories you know that graffiti is a big issue. A successful tactic has been to send out unknown graffiti. Often, someone in the community can identify the source for us. This is an example of the value of extra eyes and ears doing work for us.

CHIEF TULLY: What other kinds of information are you sending out?

SGT. LEAHY: We run the gamut. Much of the information is privileged. Anything that affects continuity of business is of interest to us and the business sector or the community. We research, vet, and clean up information that is shared. We share information on road closures, threat assessments, homeland security initiatives, and notices. One of the more unique aspects of our effort is providing travel information for the business sector. We use the Department of State advisories in preparing the information we send out. That is an added value to the security director, who is usually responsible for researching whether it is good to travel and how a given location is doing. So we provide that link and that information for them.

CHIEF TULLY: Does everyone get the same information?

SGT. LEAHY: No. We have different groups. Not everybody gets the same information. We can tailor and e-mail to a specific group, so we don't inundate everybody with white noise. For instance, if you are in the banking and finance sector and we notice a specific pattern in bank robberies, we can send that information to the security directors who can do two things. They can make their staff aware and they can take pre-emptive actions based on the pattern to protect their businesses and their branches.

CHIEF TULLY: One of the key features of the SPIN program is that you have a security advisory council. Could you speak to this?

SGT. LEAHY: During our application process, it became readily apparent to me that there is a lot of talent in the private sector. As a member of the police force, I like to think we know it all but sometimes we are surprised. The reality is there are a lot of bright people who are willing to help as long as you know how to ask the right question. Coming from a detective squad, where I looked at thousands and thousands of hours of poor video that often includes the top of the suspect's head or footage of a Superbowl party. Often I am tasked with doing an investigation based on such evidence. It is very difficult to work with. You are hanging some of your investigation on sketchy information. One of the first things I tasked the SPIN group to do was to bring in sector specialists and creating a council where we could use their expertise to improve our techniques. The benefits were twofold. One was to help me get the bad taste of looking at bad video out of my mouth. The other was, if they are going to be our partners, we need to continually evaluate what is important to them, what the business climate is, and how we can best work to meet their needs. That was the beginning of the security advisory council.

CHIEF TULLY: Mario, what are some SPIN success stories? What are the actual experiences that you have had?

MR. DOYLE: In the interest of time, I'll just highlight three of these, Chief. The State Bank on Long Island is a major institution. The security director there, Joe Crispino, displays SPIN posters of bank robberies in the back door and front door of every branch. In one of the State Bank branches on Long Island, a customer walked in, looked at one of the posters by the door and told the teller, "I know that guy." The teller, following the procedures that Joe Crispino set up, notified his office, who notified the detective squad assigned to the case. It happened to be the customer's neighbor. This was a string of bank robberies solved because of information coming out of the SPIN network that has been taken by the security director and posted in the branches.

These posters have a deterrent value to the perpetrators as well who may see their own photo at the bank entrance. Joe Crispino's approach to crime prevention is, "If I see my own face on the door, it is not a good place to go." It is brilliant.

Here's another example. An IKEA loss prevention manager, Sean Huggins, is involved in the SPIN network and is a very active supporter. He receives a lot of information on identity theft rings, credit card theft rings. Again, because of another SPIN poster display, individuals walking into an IKEA establishment were identified. The local precinct was notified and the sector car pulls up. Based on the poster information, the person wasn't arrested initially. However, information on the car they were driving was given to the detective squad to follow up through the SPIN network. The result was an arrest and the break-up of an identity theft/credit card ring – all because of information provided to the public sector from the police department.

I'll give you another quick example. Allied Security is responsible for a host of malls on Long Island. One of the provisions the client requested was that the security guards carry expandable

batons. The person responsible for the security wasn't sure if expandable batons were legal, but Allied Security's vice president for legal counsel authorized the request after checking the law. He had the foresight to call Detective Sergeant Leahy, who again researched that question. He found that expandable batons carried by security officers in Nassau County were a misdemeanor. SPIN coordination prevented what could have been a future costly lawsuit.

There are many more examples. Bill may want to cover a couple more examples SPIN benefits.

SGT. LEAHY: Some of my favorites are after-action reports, and the excitement evident generated as they are explained. I'll give you a quick example. We had a female serial bank robber. She hit six banks in the Nassau-Suffolk borders. We sent out the pattern information. The security director of a certain bank was on board with the program. He forwarded the pattern email and directed each branch manager to discuss it with branch personnel before opening and gave the managers a little pep talk about the bank robbery pattern. A particular female branch manager paid attention. That afternoon she noticed the subject, our serial bank robber, outside getting ready to come in. She announced to the group, "We are about to be robbed, everybody remain calm." She asked the private security guy to go outside and stand in the parking lot to get the plate number of the getaway car and call it in. The bank robber walked in, was told "right over here, ma'am." The robber walks up, hands the teller a note. The teller hands money to the robber and she walks out of the bank. The security guard recorded the car license plate number and called us, 911. We stopped the getaway car four blocks away. The network works well. We find that a little bit of education goes a long way. That was the seventh bank that she had just hit. It was a great success for us. Each individual network branch takes the information and steps it up to the next level.

Another really good success story shows how regional information sharing can be used. Our unit takes information and works with other intelligence centers. We have centers in Westchester, Rockland, Nassau, Suffolk, New York City and the villages. In this instance, we received a request for information on a particular blood machine that was stolen from of a hospital in Suffern, New York. It is a \$50,000 item. The hospital had no idea what happened to it, and they want to know if it might have shown up in the SPIN data base – if somebody might be peddling it around.

We have a hospital security group that encompasses the Long Island region in the New York City area. I sent the request out to the sector specific group, regarding a very specialized blood machine. Group members checked to see if anyone had come by to peddle it. Twenty minutes later I got a call from a hospital director from the Catholic Hospital Systems on Long Island who told me he was missing one also and that a partner in Suffolk was missing two. I arranged for them to talk with the investigating detective from Suffern, and they discovered that they all have

the same maintenance company. The maintenance company had recently released a person. They had never checked his credentials. They visited the guy, and there he is with the blood machines. He was shipping them overseas at \$25,000 a piece. He couldn't figure out how we found him, but within four hours he was arrested. So we transitioned from having a request for information to an arrest by using SPIN to scan four different counties. Even better, the property was recovered. That was a major success story for us.

One final example. We do our best to address local issues that may not always be homeland security or crime related. One of our members in the private sector had a son with autism. We realized that there is a lot of misinformation in the private sectors about autism including the nature of the signs and symptoms of autistic episodes, or as they call them in the community, meltdowns.

Our Security Advisory Council was able to put together a group of experts including a doctor who had been studying autism for 25 years. We were concerned about the autistic son of a local security person, who is six foot four and 250 pounds. The son's episodes are very difficult to handle. Observers mistake the episodes and response as a fight. People need to be aware that what is needed is just a little bit of space and time. The father told us the story of taking his son to a Yankee game where he went into a seizure precipitated by flashing lights. The father's necessary response involved actions that resembled a fight in the upper deck at Yankee Stadium. But a police officer recognized that the son is not really punching his father, but just trying to get away, and that the father is bear hugging his son – not fighting him. The officer asked, "Do you need perimeter? I can give you perimeter. I can have everybody stand back." The father looks up and exclaims, "Holy smokes! How did you know that?" The officer replied, "I have a nephew that is autistic."

When other officers arrived ready to break up a fight, the first officer directed them to slow down, explaining the medical situation. We saw the need for general awareness of such situations. So we put together the panel and developed a training package. We hosted quarterly meetings. We brought in experts and hosted autism training for first responders. The training was administered not only to the police, but because of the SPIN organization, we were able to offer it to the private security personnel in the malls and in the local businesses.

This effort including the panel and the training has received many expressions of gratitude, not because we are the police, but because of the results. The father has now been asked to take this program on the road. One of the first requests came from the Malls of America. They were interested in educating their security and in-house people on autism – what the signs and symptoms are, what are effective commands that will diffuse a meltdown incident. A one-word sentence can change the whole complexion of an autistic seizure. People need to be able to recognize these situations, and step back in order to create a

safe and secure area.

This is one of the programs that I am really proud of that is being used as a model to create similar programs all over the U.S. The training was available to all our members. It has been used in security guard contract negotiations where autism awareness is required for guards to be able to discriminate between fights and medical situations.

CHIEF TULLY: Ms Farber, how about you? Have you experienced any successes directly because of SPIN?

MS. FARBER: Yes. In fact, I include a success story in the opening paragraph of the article that I wrote about SPIN in the handouts. It is a success story that demonstrates how SPIN authorities and the Long Island Gas Retailers Association aided by local vendors exposed a gas pump theft operation about two years ago. Apparently it takes a key and a combination code to recalibrate a gas pump. There us a key that opens up a panel in front of the pump which gives access to a code pad. Thieves were using counterfeit keys to open up these panels. Once they gained access to the code pad, they were setting the gas pumps to go off line and then helping themselves to as much gas as they wanted.

These thefts were so seamless that in most cases the gas attendants never even realized that the gas was gone until they discovered that the tanks were missing some fuel. Initially, these thefts were presumed to be credit card scams. The real cause was discovered after a thief was arrested for using a counterfeit key and a code. Detectives then suspected that these thefts were pervasive and immediately notified SPIN. Conservative estimates indicated that, over a six-month period of time, the value of stolen fuel was about \$100,000. After our investigation we determined it to be closer to \$300,000. This would be much higher at today's prices of \$4.00 per gallon. This is an example of yet another SPIN-facilitated success.

CHIEF TULLY: Thanks, Oksana. Mr. Doyle – could you also comment on the meetings and networking that you facilitate as part of SPIN?

MR. DOYLE: Bill touched on the Security Advisory Council. The council brings in subject matter experts to help the police department - this is one important facet. The police department also reaches out to the private sector to inform them of police information priorities. Since the council's inception, we have been developing digital video surveillance guidelines which business owners are now able to use when they are bring in a contractor to upgrade their systems. There is a huge return on investment from these guidelines. Our goal was to educate the public to ensure that they were buying a product that would be beneficial to them.

We also wanted to train the public on how to use surveillance products. In many cases vendors would install their produce and walk away. We wanted to ensure that we provided guidelines

that not only taught the consumer what to buy, but informed consumers how to locate a reputable vendor that was licensed by the state. It ensured that users understood what the police department needed if his business was ever victimized by crime – what data detectives assigned to the case would need to download to apprehend subjects.

MS. FARBER: We did not want this information sharing partnering program to be a one-hit flash in the pan. We knew from the beginning that we had to establish a substantive, long-term partnering relationship like a marriage. This meant we had to start out at the fundamental behavior level. We needed to stress the desire of police department leadership to commit. We emphasized the importance of trust and honesty amongst ourselves.

Because we are in the private sector, sometimes honesty hurts. Our leadership is not command and control the way it is in the military and the police departments. Leadership in the private sector is influenced by performance and productivity. If you are not doing a good job, you're out - there is no union to protect you in most cases.

We developed a flexible think tank process. Mario talked about the needs that apply to the business owner who is upgrading his security surveillance system from a time lapse recorder system that has used the same tape for 12 years. At the same time, we wanted the police department to understand that a small business owner considers human resources and security a loss line, not a profit line. We needed to explain return-on-investment (ROI) from security upgrades. At first, the police representatives looked at me like I had two heads. So there is a great deal of information that the security and business communities are learning from each other. The most significant dynamic here is the spirit of commitment we have established. We are training our counterparts to continue in this spirit. As the vice chair of the Law Enforcement Liaison Council I have seen many wonderful information sharing and partnering programs developed across the country since 9/11 fold. Commitment and trust on both sides have been essential to the longevity of the SPIN program.

CHIEF TULLY: What would you recommend to the private sector in other regions if they were trying to initiate a partnership like SPIN?

MS. FARBER: Develop cordial and trustworthy relationships with each other. That is the biggest obstacle. Cops have to stop thinking that they know everything and businesses have to stop being security snobs and denigrating police capabilities. There are prejudices that we must overcome through trust.

CHIEF TULLY: Mario, trust?

MR. DOYLE: I think this includes developing a cooperative environment. We have talked about networking meetings. Trust is the important component. The private sector worries about their facility, campus, and environment. SPIN has created an

arena where organizations are sharing information with each other - college campuses sharing their problems with each other, hospital security directors collaborating with other about problems they have. We have opened up a venue for the public sector to share their challenges with each other, but also their resources.

Again, we all have security problems. We often believe our problems are unique to our facility, but usually they are not. We now can share information on problems and solutions with the police department and other businesses to gain valuable advice, guidance, and support. Trust has been the foundation of this program. By vetting the membership, we established a level of trust from day one. We have established an environment where we can speak to each other freely and not worry about our information being on the six o'clock news.

CHIEF TULLY: Bill, what has been your experience?

SGT. LEAHY: Yes, it really is about trust. For me, it's stepping outside of the traditional police role to recognize that, through broad-based communication, we can solve a lot of the issues that we perceive as sector specific. I've found that if we place an issue in front of the larger group we get better solutions. The beauty of our program is that it is cross-disciplinary - not sector specific. In our meetings, the networking opportunities and ability to address a question as a group are beautiful things to see. On a problem encountered by a given business, a SPIN partner often indicates, "I have already been through that. Come see me after the meeting. I can give you the information; I can give you the resources." We are a resource-rich group. Members don't need to handle an issue alone.

We blind-copy our e-mail groups to protect our mailing lists. When someone asks us a question, we turn it around to the group as a request for information. Based on responses, we then marry the requester with the solvers. This process alleviates a lot of angst for some security directors and makes them look good to their management as problem-solvers with reach and ability to solve problems in a timely fashion.

CHIEF TULLY: I have a final question and then we'll open the forum up for audience questions. What about the future? How do we take SPIN to the next level? What does the future hold for SPIN?

SGT. LEAHY: It would be good to have a bigger budget. More specifically, I would love to see us develop a web based portal where we can archive our information and create chat rooms for the sector specific groups and the general SPIN membership. That will be an important next step. That would require adding IT support, an extra person, maybe a webmaster to enable us to continue to vet existing information, clean it up and decide what is important to save.

I also think it will be important to create a text messaging group so that we can send out quick short bursts of information - targeting

high school and college kids where text messaging is the prevalent form of communication. That is another group that we are looking to reach by tying in the crime stoppers program with a text messaging address. By doing this, feedback information can be returned to a crime stoppers program.

Discussion with the Audience

CHIEF TULLY: I would now like to open the floor to audience questions.

PARTICIPANT: It is fascinating. The SPIN network has grown into a well-greased system that is part of your daily routine. Are there sector specific plans that provide guidance related to vetting the information that is distributed to the sector specific groups through the network? Is that information reliable? How much real time information sharing is going on among and within the groups outside of the SPIN network? How are you vetting or controlling that information? Or are you assigning people to try to disseminate that?

SGT. LEAHY: It is. We are lucky enough to be a police department that has an intel center located across the hall from us. They are my favorite customers. We use them extensively. Plus, we are reaching out to other agencies. We get reports in from many organizations. It is imperative that my staff go back out, call that person up and try to find the source of the information. We are oriented to finding the source of the information, then giving them credit if it is good information. Regarding sector specific information, if you are part of our critical infrastructure, you are a vetted group. As such, you get a different level of information than if you are the Kiwanis Club. As far as control, information sharing and assistance is based on need, mission and how the organization relates. For example, utilities will get a different level of information than the PTA members.

Our information sharing process is tailored and specific when it needs to be. For the all crimes-all hazards process, we use more general information. I find that we feel safer if we put a label on something. If I stamp a document "law enforcement sensitive," I'm done and I'm safe. Often that is an impediment. Our job is to go through sensitive material and determine what things we can leave out and still get a useful message across. I can leave investigative information out and still get a message out that allows people to look for the information I need. We work together with the squads, the specialized units and the other agencies.

CHIEF TULLY: It is annoying when you see material stamped law enforcement sensitive that just appeared on Channel 2 on-the-scene TV coverage.

SGT. LEAHY: Sitting on a skiff and watching CNN as your encrypted message comes over.

PARTICIPANT: Has SPIN improved your real-time response?

SGT. LEAHY: Yes, we've seen some improvement. We are often pushing it. In our office we have radios that are listening to the crime trends and the calls for service real time. Then we have the computer aided dispatch on our desktops. The officers are basically peering right over the shoulder of the officer at the scene with the dispatcher putting together the information. If a bank robbery occurs, within a minute of the initial description, that information has gone out. If an incident involves a major road closure where we need crime scene and homicide detectives, that road closure order goes out within a minute. If there is a suspicious activity going on, we can take that information, look at it, review it, and within an hour turn around and send it back out to a specific group asking for any needed clarification. Often this involves asking the organization to review their logs to check if they have seen an offending vehicle or person before.

DR. KLAU: How would you rate the SPIN program in view of deterrence? Have you seen a reduction of certain crimes and incidents, as well as keeping the general public informed and giving them an improved sense of security?

MR. TULLY: We are very proud of the crime rate in Nassau County. Our rate has been consistently low for the last few years. In fact, the crime rate in Nassau County is the now lowest that it has been in 40 years. We are ranked number one in the nation for the lowest crime rate in populations over 500,000.

MR. DOYLE: From the private sector standpoint, deterrence occurs because we are better prepared. Bill talked about SPIN enabling us to instantly send out a notification of a bank robbery. Our preparedness is also facilitated by the police departments sending us the image of the bank robber as soon as possible on the same network. As we have experienced, the photo may be distributed the same day the robber plans to hit six banks in a row. Now the targeted banks are armed with warning information. From a private sector standpoint, the value, whether it be hurricane preparedness, bomb warning, you name it; having timely information for events on the horizon helps us prepare for and, in many cases, prevent disasters. For instance, on Memorial Day weekend, we receive safety-related information. We are surrounded by water, so boating safety reminders are helpful. The SPIN information network prepares the community for current problems to watch for and tools and procedures to provide feedback to law enforcement if needed.

CHIEF TULLY: I need to clarify our program's relationship to the general public. The SPIN network is geared for security directors of organizations such as banks, hospitals, schools, superintendents of schools, vulnerable entities, and PTAs. Security leadership must relay SPIN information to their constituencies to get the general public involved.

MS. FARBER: I have two examples of how SPIN has helped tremendously with my business and my employees. One of the gentlemen in the police department's SPIN office mentioned to me that some of the SPIN members were tired of getting traffic alerts. I informed him of their value to our manufacturers'

truckers in avoiding accidents and congested routes. I asked him to keep up the good work because the alerts have made a big difference to us in getting products to customers in a timely fashion. We have also found the SPIN information on gang activity to be very helpful. It is a huge problem in this country. We find gang alerts helpful to our immigrant warehouse workers in identifying and avoiding gang areas. Yes, in answer to your question, I do believe as a professional that it has cut down on crime.

SGT. LEAHY: We have anecdotal stories about prevention. We laugh about Joe Crispino and his crime prevention, but that was a quote from a bank robber - "If I see my face on the wall, I'm not going in there." That is a great example. One of the other examples is that one of our SPIN members has a large commercial warehouse and moves millions of dollars of product every day. He wasn't very well versed in gang activity and gang identifiers. He thought that his local forklift operators all belonged to the farm club because they all had red bandannas hanging out of their pockets. We did a presentation for his business on gang identifiers and gang activity in the country and in the region. He said to me, "I had no idea that meant they were flagging. Now I know that term, so I'll have to get rid of my farmers." At that time, he had a theft problem in his warehouse. Also, there was gang-related graffiti in the bathroom he didn't understand, but it was gang related graffiti. As a result of our presentation, he conducted an internal investigation and found that the crew was cleaning out his warehouse. In reviewing new applicants for the warehouse positions he noticed that certain letters were crossed out on the forms. He now knew that this behavior is related to gang culture and identification. Based on the crossed-out letters, he can tell that many of the new applicants were members of the same group and informs them, "You are probably not right for our job." Many of the benefits of SPIN we learn anecdotally, but wouldn't show up in crime statistics.

MR. THOMAS: I'm Dutch Thomas, consultant in national preparedness. How do you make a distinction, or do you make a distinction, between "information" and "intelligence?"

SGT. LEAHY: That is a great question. We use our intel center to break down incoming reports. As you are well aware and I'm sure this group is, "information" is raw. When we started, we liked the term "SPIN information network" instead of "intelligence network." One of the reasons for that is because "intelligence" connotes data that is law enforcement sensitive and can exclude people. It is semantics but it is a stumbling block. We vet our information before we send it out. We utilize a lot of the current criteria through the FBI crime analyst work and our intel centers.

CHIEF TULLY: Is there a final question?

PARTICIPANT: Could you describe a little bit more about the relationship between your work and the intel center? How is information passed?

GT. LEAHY: It is an open relationship. One of the things that we have been able to do over the years is to institutionalize the SPIN program within the police department. They recognize it is not a flash in the pan, it is going to stay, and they value it. It is incredible that even in an intel center, we may not know who to reach out to in the private sector to find certain information. We fill that gap. Our relationship must be two-way. We all operate under the same umbrella as the Nassau County Police Department, so we want a good product to come out.

Our relationship is back and forth, walking across the hall. "I am looking for this information, can you get it?" Some of the information that we use is from institutions that compile great position papers and written information that we break down for a local level. In such cases we cite the original source and explain how the information applies locally. That is how we use intelligence.

MS. FARBER: If I might add - in the beginning we spoke very openly to each other about blunt questions. I told SGT Leahy, "SPIN is such a great program, how do the other cops feel about it?" He told me bluntly that they hated it. So the police buy-in and the intel center's buy-in took awhile. But it is now operating well, effective, and cooperative.

HIEF TULLY: That concludes our panel discussion. I hope it shed some light on our program. Once again, I want to extend my thanks, and I'm sure the panelists do the same, for inviting us to speak.

MR. KNICKREHM: Thank you very much, Chief. We are coming up on break. We have included evaluation sheets in your printed programs. Before you leave, please do us the favor of filling those out carefully. This year's theme, fostering public-private partnerships, came from the feedback that we got from the audience at last year's symposium. So we really do read these things and pay attention to your comments.

Panel Two: All Hazards Consortium (Regional) Panel

MR. KNICKREHM: Ladies and gentlemen, it is now time for our second panel. In this panel we are moving up a level of complexity in public-private partnerships, from the local level to the regional level. Our regional panel is moderated by the Honorable Robert Crouch, who will now introduce both himself and his panel.

Remarks by Hon. Robert Crouch

MR. CROUCH: Thank you very much. I am Bob Crouch and now serve as Governor Tim Kaine's homeland security advisor. In Virginia we refer to our homeland security endeavors as our system for "Commonwealth preparedness." For the last year or so, it has also been my honor to be the president of the board

for the Mid-Atlantic All Hazards Consortium. What we would like to do with this panel is tell you a little bit about the work of the Mid-Atlantic All Hazards Consortium, how it was created, how it benefits the various partners, and what our vision is for the future.

I am joined this morning by three very strong supporters of the All Hazards Consortium effort. To my immediate left is David Lindstrom. David is with Penn State where he serves as the chief privacy officer, the EMS academic programs coordinator, and the Homeland Security Coordinating Council member for the university. David has been a member of the board for several years and a very active participant in all of our efforts.

To David's left is John Contestabile, with the State of Maryland. He is the Director of Engineering and Emergency Services at the Maryland Department of Transportation. John is one of the founding fathers of the All Hazards Consortium effort. One of the things that he will share with you is the history of the initiative. John is also the state interoperability coordinator for the State of Maryland. That is an area in which we have all been actively engaged.

Then finally, last but not least by any means is Mike Hughes. Mike is the Northeast Program Development Manager for Northrop-Grumman Corporation. You can see from my introduction of our panel that our partnership involves government, the academic community, and the private sector. Mike has been a very strong supporter from the private sector and a very strong partner with our all-hazards effort.

As we go forward with our presentation, each panelist will address how our regional consortium effort has benefited academia, government at the state level, and the private sector. It is very much a partnership – that is our vision. The chart that you see above us [insert chart] presents an overview of the All-Hazards Consortium. I won't read that, but will leave it there as context reference for you. I will be speaking from observation experience.

We are a partnership within the Mid-Atlantic region. We involve eight states from North Carolina to New York and the District of Columbia. Participating states include North Carolina, Virginia, West Virginia, Pennsylvania, Delaware, Maryland, D.C., New Jersey and New York. Our board has representatives of state government for each of those states, as well as representatives from academia and from the private sector. We have a number of universities, including the co-host of this symposium, James Madison University, which has been very engaged in our efforts, and we value that participation very much. We certainly applaud James Madison for its efforts in the preparedness arena.

We take an all hazards approach to our effort. Our philosophy is, by collaborating together across state lines and across the private and public sectors and with academia, we can come up with better solutions that will benefit all of us. We all have a tendency to be very focused on our immediate concerns and

immediate needs within our jurisdictions, but most often the issues that challenge us are issues that our counterparts in other states face. We can learn from the best practices developed in each of our member jurisdictions.

There are certainly many other vehicles that serve a collaborative purpose. The National Governors Association, for example, has a Homeland Security Advisors Council. We gain benefit from that. There are other organizations like the National Emergency Managers Association. In our individual roles, we network with other associations and organizations and meet with our counterparts from other states. But the All Hazards Consortium is unusual and perhaps even unique, in that it brings the state government folks, the academic folks and the business community together. We greatly appreciate the opportunity to be with you this morning and a chance to highlight the organization and benefits of our regional partnership.

I was struck by the earlier panel. It was abundantly clear from the discussion that the panelists really believe in what they are doing; that the local partnership is highly beneficial and something they are very committed to. They see that it is making a difference in their communities – there was genuine enthusiasm. You will also find that that is the case with our panel. We are all very committed to the All Hazards Consortium to the point that we treat it as a second job in many respects.

There is tremendous camaraderie that has developed over the four or five years of the consortium effort and that is part of the value we have gained from it. Before John kicks off our discussion with a little bit of the history and the structure of the organization, I want to highlight our program over the eighteen months since our inception. Over this period we determined that one of the ways for us to gain most value from our collaborative efforts would be through a series of workshops.

In January 2007, we had a fusion center workshop hosted by our colleagues in Trenton, New Jersey. Representatives of the fusion centers from all of the participating states attended. One slogan that we have in the consortium is to “be responsive to those who own the problem.” So, for example, it is most typically our state police personnel who manage our respective fusion centers within the states. But the fusion centers are a fairly new development, a new dimension in information gathering and sharing among law enforcement and emergency responders. There are different levels of evolution of these centers. So getting all the fusion center people together in the Mid-Atlantic and developing networks that they could then build on spurred progress in the development of these centers. One of the things that we do with each of the workshops is to produce a white paper on issues and solutions. Our corporate partners have been very supportive in helping us develop these. We have been sharing these with Congressional staff and others.

We followed the fusion center workshop with a communications interoperability workshop hosted by James Madison University in Harrisonburg last May. In the summer, we partnered with the

State of West Virginia in a catastrophic planning and evacuation and sheltering planning workshop that was built upon recently by a follow-up effort in Shepherdstown, West Virginia. You will hear more about that collaboration on catastrophic planning as we proceed. In October, Dave Lindstrom was kind enough to host a critical infrastructure protection workshop at Penn State. So we feel that the workshop effort that we have undertaken over the past 18 months has added an extremely valuable and new dimension of our All Hazards Consortium efforts.

In summary, our All-Hazards Consortium membership includes eight States and the District of Columbia. Our efforts involve the homeland security advisors in each state, the emergency management directors in each state, as well as other participants from government and private partners and academic institutions. Our effort has been underway for a little over four years. John Contestabile, from the state of Maryland, has been involved from the very beginning. I will now ask John to tell a little bit about the history and the organization and how we work in collaboration.

Remarks by John Contestabile

MR. CONTESTABILE: Thank you, Bob. I don't know, but I suspect that I get to do the history part because I am the oldest up here. I have certainly been around state government some time. I spent 30 years with the Maryland Department of Transportation. It has been interesting. I did a stint as the Deputy Director of the Governor's Office of Homeland Security in the previous administration, so I have been involved with the emergency management function since 1996, and homeland security since 9/11/2001.

When I was the acting deputy director of the Maryland Governor's Office of Homeland Security, a fellow by the name of Dennis Schrader was the homeland security director at that time. Many of you may know Dennis. He is now at FEMA as Assistant Secretary or Deputy Administrator. At that time, Dennis had attended some events with George Foresman who was one of Bob Crouch's predecessors. One of the events was in Virginia - a homeland security summit or exhibition with the private sector. Dennis came back charged up and said, "We ought to do something like this in Maryland."

At that time I was working in the area of interoperability and chairing Maryland's interoperability effort. We were trying to work with our private sector partners in achieving interoperability. We were concerned that the worst thing we could do in our approach to interoperability would be for the government to come up a plan that is not informed by the latest technology. We recognized the need to find a way to reach out to the private sector.

So in terms of the history of the consortium, there were a couple of things occurring that fortuitously coalesced at a critical point in time. In most cases an organization begins and later its members see the need to have an annual meeting or summit. Our organization is an example of the converse. We conducted an annual meeting before we had an organization. You may

have heard of the All Hazards Forum. It is an event that we have held for four or five years at the Baltimore Convention Center. This follow-on to the Virginia homeland security summit, married with the public-private partnership formed because of our interoperability efforts, led to the All Hazards Forum.

The All Hazards Forum is a mile wide and an inch deep. We have 30-odd technical sessions. We cover everything in homeland security from evacuation, to pandemics, to the health and medical side, and transportation issues. It took a couple of years for the forum to gain momentum. At that point people saw the need to drill down a little deeper, especially in the area of interoperability. We also saw the need for some sort of framework to sustain our efforts throughout the year, rather than activity spiking during our annual meetings.

So we progressed from the annual forum to create an organization we call the All Hazards Consortium. We now coordinate with and support efforts of our nine member states on a year round basis. Establishing the consortium has been very gratifying. We have developed bylaws and appointed a board of directors and advisors. It took a lot of work over the period of a year to stand up the organization. So we turned our annual forum event into the All Hazards Consortium organization. The consortium then organized the workshops that Bob Crouch mentioned. We have sponsored four or five workshops so far. In fact, we have one coming up in July, a GIS workshop which will be at Towson University in Baltimore.

Our method is to find the people who own a particular problem. Our strategy is to work at the senior level as well the practitioner level. We think that is important because we want to be able to survive turnovers in administration, which is inevitable since we have government leadership involved in our board. The board's senior representation includes homeland security advisors like Bob and the EMA directors. These folks are very helpful in providing direct links into the governors' offices. But we also find the practitioners who own the problem. We include the interoperability coordinators and we bring them together using a series of conference calls. We also hosted a workshop on interoperability to drill down that subject in some detail. The workshop product is a white paper. We also host periodic regional and state association meetings. See figure one for highlights of our year round programs.



Figure 1

We have several expressions within the consortium. One of them is: “we like to connect the dots, but we don’t want to be a dot.” That is important because there are a lot of associations out there, a lot of groups doing really good stuff. When we come alongside them, we don’t want them to think that we are going to steal their members or that we are going to somehow compete with them. Our mission is more virtual -- to connect the dots so that the left hand knows what the right is doing in order to facilitate information exchange and coordination among our members. In the context of interoperability, our expression is: people, process and technology. The consortium pays particular attention to the first two items: the people and the process.

What do I mean by that? I mean making sure that the left hand knows what the right hand is doing. If Person A doesn’t know person B who is A’s counterpart in the next state over, we can’t have consensus on what to do, how to collaborate, and how to work. We bring together the people who own the problem and put them through a process of conference calls, workshops and a white paper with approved recommendations on how to move forward together. It is only after we have addressed the people and process issues that we are in a position to plan for and implement technology or technique improvements. Many of the problems we see with other programs are due to lack of focus on people and processes across states, across jurisdictions and across disciplines.

I belong to a lot of organizations and they tend to be discipline specific. I am an engineer by training, so I belong to the American Society of Civil Engineering. It is great, but it includes only engineers. So we saw the need for an organization that would bring together fire, police, law enforcement, transportation, public works, and public health disciplines. I know am preaching to the choir, but the challenges we face in homeland security are such enormous, interdisciplinary challenges. You look at evacuation planning or any of the topics Bob just mentioned: evacuation planning, interoperability, critical infrastructure protection, or fusion centers. These are huge problems that obviously require working across jurisdictions and across disciplines. We look around and we see a lot of organizations that are discipline specific or jurisdiction specific. I don’t want to sound like I am knocking those organizations because they address important needs. The All Hazards Consortium was born out of the need to bring public and private sectors together along in a multi-discipline framework.

The last panel used a really busy slide. We have to have a really busy slide too showing how the AHC works. The basic ingredients are the people, the process and the outcomes (see figure 2). The process is an annual rotation starting with the All Hazards Forum typically in the fall. We cycle our meeting locations among the private sector, the universities, the not-for-profits and the other organizations. We have a basic, collaborative year-round regimen. Here are some of the outcomes: relationships and partnerships, regional collaboration, a shared vision and

strategy. We are working towards applied technology. Our white papers have addressed MOUs, coordinated procurements and improved regional readiness.

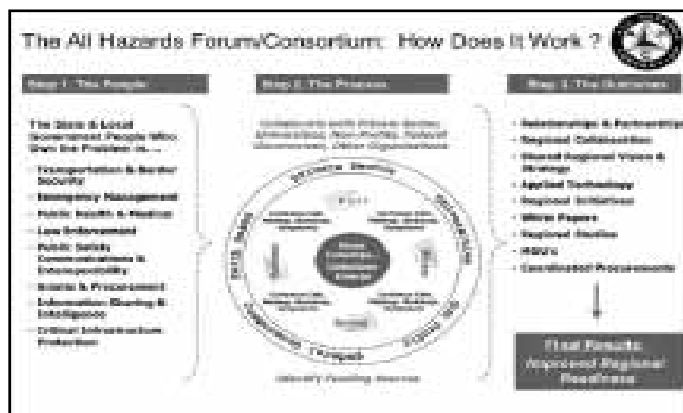


Figure 2

I can’t overstate the importance of staying true to your core beliefs and vision. In any organization, it is easy to get off track. Our core focus is the real problems that our member States have in homeland security and emergency management. Our job is to solve the problems that the states have on a collaborative regional basis. If we stay focused on the problem and we stay focused on solving those problems, then the corporate partners will be there, the government people will remain interested, and we will get results.

My final slide illustrates where we are now and where we are going in the relative near term. As I said, there has been an evolution from the forum as an event to an organized consortium conducting problem-solving workshops on specific topics and producing white papers. At present, we are taking the recommendations in the white papers and working with our partners to generate project proposals that will attract funds for real work to solve the problems we’re facing. The chart illustrates this (see figure 3). We are identifying regional initiatives, fleshing them out, and then developing related grant or funding requests. We’ve had some success. For funded proposals, we perform the effort and report our progress through the All Hazards Forum. For each project we report objectives, approach, findings in terms of best practices and lessons learned, and next steps. We are excited because we are bringing new resources to the state. In this regard, the AHC is a well paying second job. We are bringing people from the private sector to combine their expertise with the public sector principals who own the problem. Another maxim we use is “We give voice to the people who own the problem.” I know from experience as a longtime government employee, that these people spend many restless nights wondering how to solve the hard problems such as interoperability or large-scale evacuation protocols.

The people who own and work these problems are senior career people in the different agencies. We find those people in each of the states and give them a platform – an opportunity to tell

their story, meet their partners in the region, and collaborate on a solution. In the past, each state did its own thing and, in many cases, made the same mistakes as other states. The All Hazards Consortium provides synergy and traction because working together energizes people to work harder. The private sector is happy to be a part of this process because they participate directly rather than standing on the sidelines.

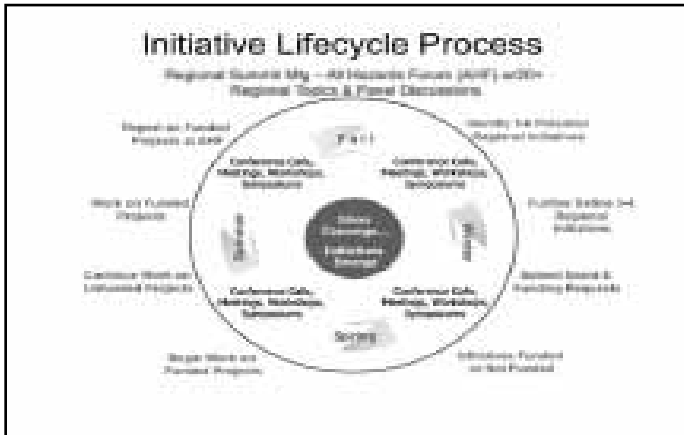


Figure 3

My final point is that we know how to deal with the private sector. We work with the private sector from three perspectives. I must give George Foresman some credit for this idea. We deal with them as a victim - it is their business that may be damaged in a disaster, they are part of the Stafford Act relief and Small Business Administration rubric. We deal with them under contracting and acquisition regulations and ethics rules. And we are now learning to deal with them well as a partner. We often talk glibly about public-private partnerships – but making a public-private partnership work is a real challenge. We must determine where the public interest lies and where the private sector interest lies and discern the certain area of commonality and overlap. But there is also an area where we diverge - where we part company. Recognizing that and walking through that is a challenge. Nonetheless, our relationships within the consortium have matured to the point where we are working closely with our private sector partners. I hope that my presentation of the history and operation of the consortium has been helpful. I yield the floor back to Bob Crouch.

MR. CROUCH: Thank you very much, John. I would be remiss if I didn't mention that one very valuable partner in all of our efforts who has been there from very much the beginning is our executive director Tom Moran from Maryland. He comes out of the private sector. Tom had a family graduation today that prevented him from being with us, but he is really a great champion of this effort. We would not be anywhere near where we are in our efforts without Tom's efforts to keep all of us pointed in the right direction. And now I would like to call on Dave Lindstrom for the academic perspective, and then we will turn to Michael.

Remarks by Mr. David Lindstrom

MR. LINDSTROM: For 36 years -- I just figured it out as I was sitting here, much to my chagrin -- I have been employed by someone or something related to higher education. Many of you may be in higher education, since this symposium is co-sponsored by a very fine university. Please forgive me for anything that I say that offends you. And you will see what I mean. I started my career in the business of training people in emergency medical services, and was hired as a faculty member at Penn State 32 years ago. I had planned to stay in academia for two years but my plans didn't work out -- I got stuck. Within the university, I have had operations responsibility, emergency management responsibility, clinical responsibility, patient care treatment responsibility, and all kinds of bureaucratic positions within the university. At present, I have largely compliance and regulatory responsibility -- but I have kept my hand on the homeland security space because of my passion for it.

Penn State put me on a cooperating council because, as you know, in a big university like ours with 16,000 employees and 85,000 students, there are so many cooks in the kitchen. People often ask me "You're at Penn State? Do you know this guy who's world famous?" In most cases I haven't a clue. I may have seen him at the gym but the University is so big it is hard to keep track. It's almost like working for the federal government.

We have many homeland security related initiatives -- I just wrote a few of them down. They include port security, provider education, data fusion, an extreme events lab, a number of related bachelors' degrees. Our newest is a degree program in forensic science. I was a deputy coroner once. I keep wondering where all our graduates are going to get jobs. But they do quite well. We also are developing professional masters' degrees in the homeland security emergency management. The latest is within our College of Medicine in the public health space. We are also deeply involved in GIS, and geospatial intelligence.

The University is a very interesting place to work. My job is to look at our programs in an integral sense to figure out how can we best help society. This is my challenge, my concern. You may be surprised to learn that this is not a concern generally shared in higher education.

Institutions of higher education have various missions to perform that are very important. We have an academic mission which includes three or four parts, depending on the University: education, research, community service, and government service. Penn State's missions are manifest in many different programs. We are a land grant institution. We have responsibilities for homeland security in the agricultural space. The mission which most people think of when they consider higher education is training people to do something. This is a huge part of our mission, and a very important part of our infrastructure. But this isn't the aspect of our mission that gets the real attention behind our exterior ivy-covered doors. Rather, the mission aspect that

gets the most attention is research. Research is the measure of how we move forward as a society, as an academic institution, and how we move towards solving problems.

The problem that we face as a collaborative organization is that we need rapid solutions to the problems we face. In most cases, we don't need years of research. We need to find of the optimum types of tunnel monitoring systems, the optimum types of port monitoring systems, which sensors are appropriate for a given application, and how we might turn everybody into a sensor monitor using their cell phones. There are many things we can do with existing technology without spending years on research and development. Based on my 36 years of experience, a major challenge is to set up our projects to ensure accountability and a useful product delivered on time.

In many ways, I feel like a mole. I am in higher education. I am proud to work for a wonderful institution that does some really great things. One of my jobs and one of my purposes for becoming a member of the AHC is to do exactly what everybody has been talking about -- to get in touch with the people that own the problems and determine who in the university might have applicable expertise and resources that are affordable. University research tends to be affordable. We don't have big profit margins and we have a public service responsibility. We have a large labor pool of relatively affordable people, especially if we can use students and graduate students. We don't have a vested interest in the long-term outcome because we are normally to turn product implementation over to a private sector partner. Most universities, including Penn State are not in the business of competing with the private sector.

One of our challenges is how we bring the massive power of a higher education to the table across the United States. Certainly research dollars interest universities. If universities see possible spinoff research opportunities, then they tend to be interested. It also helps if the project can be tied to the higher education curriculum -- to prepare professionals to work in a critical subset of the homeland security enterprise.

Universities have roles in community service and outreach, both professional and undergraduate and graduate education, and research. But universities must be in touch with what is actually going on. JMU is certainly an example. They brought us all here today. They have some very good efforts moving forward, as do other higher institutions in the region and elsewhere in the country. As a result of some of our workshops there has been an interest generated, spurred by the Commonwealth of Virginia, in campus safety and evacuation planning. So that is another piece that has emerged. One of our goals within the All-Hazards Consortium is to encourage more universities to engage in the homeland security enterprise.

My ability to get Penn State involved resulted directly from my participation in the Forum and the All Hazards Consortium. Were it not for the exposure that happened because of police, fire, EMS, emergency management, academia and the private

sector working together within the Consortium, our university's connection might not have occurred. So I see the All Hazards Consortium as a success story in the sense that bringing us together was crucial in creating critical mass that has enabled difficult concrete solutions to homeland security problems. I contend that higher education involvement in research and testing has been very productive. It has worked well in that we are engaging private partners so that when the project is completed we have a partner with a vested interest, a commercial appeal mission, to move our projects and their products to the field.

Remarks by Mr. Micheal Hughes

MR. CROUCH: Thank you, David. You have provided a good segue to our next panelist --Michael Hughes from Northrop Grumman. Michael has been a highly committed participant in the All Hazards Consortium activities. He has attended each of our workshops over the past year and a half. Mike will provide some perspective on the role of the private sector in the consortium effort, and what they gain from it.

MR. HUGHES: First of all, I would like to validate that the model does work. When Northrop Grumman first started participating, I think we had one, maybe two private sector members. At the last forum, we were turning away corporate folks, vice presidents, and directors because we had met our limit of 12 private sector representatives coming to the Forum.

Northrop Grumman sees the All Hazards Forum as an extension of our marketing communications efforts to enhance our existing relationships with clients and to help us to develop new relationships for information sharing. When John talked about the stakeholders, the decision makers and the solution providers being in the same room -- sitting down and listening to the challenges and the priorities -- the private sector is in a listening mode. It is very helpful to us to hear the incident commanders and the first responders speak freely and openly about their issues and concerns and how they would like to move forward.

One of the things that we introduced to All Hazards Consortium was the vision sessions and the white papers. Northrop Grumman sponsored the first Fusion Center White Paper. We were amazed at how many folks from the region were able to attend, sit down for a full day, and rotate through three different sessions, each sharing their needs, requirements, issues, concerns, challenges and priorities for fusion center development. To be honest with you, we had four or five subject matter experts and facilitators in each session, and they were just blown away at the openness on the collaboration side concerning some of these issues.

We were able to identify someone inside of our organization -- Joey Booth, who was the incident commander for Katrina, to sit down with all of the documentation and go back and talk to the participants, the stakeholders -- the people who really owned the problem. Mr. Booth then produced a document that everyone looks upon as a major resource to help folks go forward with their fusion center development.

Our corporation really appreciates the way the All Hazards has been providing its services. We are a big supporter. The bottom line is that we are interested in what keeps our customers up at night. John spoke about people, process and technology. We are there to listen and support the effort because we want to help provide some of these solutions. From a marketing and business development standpoint, it helps us shape, and what I call “rack and stack” the business opportunities based on what we are hearing from the end users concerning how they want solutions deployed in the field.

Panel Discussion

MR. CROUCH: Thank you, Mike. Let me now start the questions to the panel with this one. One of the things that first strikes people and perhaps confuses them a little bit about our relationship is that we have Northrop Grumman and other corporations as very strong supporters. People ask if these participants come away with contracts. Does their involvement with the consortium give them some inside track with government? As this has developed we have all been concerned about potential conflicts of interest. Earlier, John mentioned the procurement process that we all adhere to. The ethics piece is a concern for each of us, whether our perspective is private sector, public sector, or academia. Mike, how do you view that? Do our private sector participants come away from the process with contracts?

MR. HUGHES: No, we don't come away with contracts. What we come away with is a level playing field for all of our business partners. This enables us to engage at the right level of interest with the appropriate decision makers and stakeholders. The reason why this is so important is that there is a lot of technology out there. Your concept of operations, your governance are crucial to determining which technology to use and how that technology needs to be deployed to give the government well-rounded solutions that will really help the region.

We don't look at the All Hazards Consortium as, “where is the beef, where is the contract.” We don't match our return on investment dollars to sales simply because there are other means of market intelligence that help us to identify the funding profile. What we are really interested in from this relationship is helping the customer to get on the right page and helping stakeholders to agree how to do forward.

MR. CROUCH: Is that a fair statement?

MR. CONTESTABILE: I would also add that maybe in the early days of the forum and the consortium, when you had the private industry sales side of the organization fully engaged, there was a misperception that the consortium was about marketing. What we have found over time, and it has been a learning process on both sides, is that our corporate partners began to engage on multiple levels to the consortium. For example, certainly you might have the sales and marketing team there, because they need to know who the decision makers are and they need to know who their customers might be. But then we also began to

see people like the VP of new product development attending because they want to know what the need is for the next product that they have to create. We are also beginning see the VP's for corporate security. In Maryland, if we have a plant from company X that employs 3,000 people, the director of corporate security wants to know who the EMA director is, and wants to know how the fusion center is sharing information. So we are starting to see corporate security types coming to our events.

So it has been interesting because our partners have begun to see value in the consortium at a lot of different levels, not just from a sales and contracting perspective. The consortium is not so much about specific sales opportunities as it is getting some consensus across the people who own the problem as to what we ought to be doing and where we ought to be going.

MR. HUGHES: Business-to-business partnerships are being fostered and developed, centered around topics like critical infrastructure protection, public safety communication, health and human services. Those broad topics allow us to develop a framework for the stakeholders to go forward. That is really important. From my standpoint on the business side, the last thing I want to see is an RFP or a task order come out that is not framed properly, or it doesn't use the latest and greatest approach. The All Hazards Consortium, through the vision centers and the white papers, has used the best practices and lessons learned from regional deployments in their planning on how to move forward. The business-to-business aspect is very important. Working with our colleagues and universities is very important because they have far more intellectual capital than we do with respect to the best and the brightest. We go to them quite often for partnerships and relationships to determine how best to deploy solutions. So it works quite well across the board.

MR. LINDSTROM: If I could add a higher education comment, I think one of the challenges for all of us is that engaging and listening and learning takes a lot of patience. One of the problems in our business of higher education is being patient and engaged enough to hear what is being said before responding. Often, people in all sectors want to go to a meeting just to receive information, figure out what is going on, and move away with their own, often half-baked plan. One of the strengths of the information that emerges from this consortium is that it is processed and not just an unvetted handout from PowerPoint presentations. It requires staying engaged. And Penn State has been very good about letting me stay connected to the forum and supporting my activities with no stipulated return on investment other than to sit at the table and learn from the collaboration.

MR. CROUCH: Let me give an example of a process where the consortium played an important role. I think probably everyone here is familiar with the annual Department of Homeland Security grant cycle. In the 2006 cycle, Maryland, Virginia, West Virginia and Pennsylvania were encouraged by some parties at DHS to submit proposals. I am not trying to be critical of DHS here --

they have gone through an evolution as a young department, just five years old. This example of how the consortium has helped illustrates is that DHS has listened and thus improved their process. The four states which meet along the I-81 corridors up around Winchester, Martinsburg, and Cumberland were encouraged in our annual grant cycle process to include an investment proposal which we called the quad state interoperable communications effort. The proposed effort included shared planning and baseline assessments to encourage interoperable communications in that quad state region. One voice at DHS was encouraging all four states to submit these matching investment proposals. Unfortunately, the evaluation of the grant submissions was done by an entirely different office that wasn't aware of precursor events -- our proposals were rejected. Our reaction from the four states of course was some degree of indignation. Using Michael's term, the All Hazards Consortium served as a "framework" for us to collectively approach the appropriate parties at DHS. We informed DHS of the need for a mechanism written into the DHS grant guidance that not only permits but encourages multistate proposals since collaboration enables shared benefit. I am happy to report that DHS listened. In the 2007 cycle, last year, they did have such a provision that benefited all states and the entire nation. It grew out of the All Hazards Consortium's quad state proposal experience and subsequently voicing our concerns DHS. The rest of the story ends happily -- last we received funding for our multi-state interoperability effort. The funding applied to all of the FEMA region three states within the All Hazards Consortium and supported multi-state catastrophic and evacuation planning. This instance of the All Hazards Consortium serves as a voice for the states working together with a federal department has been repeated. John Contestabile will now explain the recent dialogue that the consortium has had with the DHS Assistant Secretary for Infrastructure Protection, Bob Stephan.

MR. CONTESTABILE: Every state has an obligation to implement critical infrastructure protection. We are on the receiving end of federal Presidential directives, grant guidance, the federal Response Framework, the National Response Plan. As states, we are required to understand and comply with national homeland security strategy. But what does CIP mean? How do we do this? What does successful CIP look like? The federal offices that are developing the strategy don't operate the systems that we operate. And every state is a little different in terms of its mechanisms. So the states have to do a lot of translation to be able to implement the strategy requirements. Because of the difficulties associated with strategy implementation, we organized a workshop. The consortium makes a concerted effort to identify the problems that are causing the most difficulty for our member states. CIP was a problem. So we held the workshop at Penn State.

To Bob Stephan's credit, he accepted our invitation to attend. Oftentimes, if federal partners attend conferences or other events, they'll stay long enough to deliver a keynote address. Or they may come in for lunch. To Mr. Stephan's credit, he was

with us for the duration of our workshop. He stayed for two days. He came for the pregame, too. I spoke with him expressing my thanks for the time he invested in our workshop and directly engaging with our group during the event. His response is really telling. He said, "How can I not be here? When nine states get together to talk about something that is in my portfolio, I have to listen." He sat the audience and took notes. During the coffee breaks people button-holed him and asked him on many specific issues. It is a great example of what the consortium is able to accomplish by creating the platform and the framework for the people who own the problems at all levels of government to work together and get results. We have been very pleased to see our federal partners participating in our events.

MR. CROUCH: We also had DHS participation at our catastrophic planning session in Shepherdstown, West Virginia earlier this year. John Serubi, the regional administrator for FEMA Region Three out of Philadelphia, was there both days. This is something we greatly value. We benefit from their presence at our meetings because they lend credibility to our efforts. And the federal agencies benefit because we serve as a vehicle for them to achieve their regional planning and implementation goals.

Thus far we have talked about interoperability and fusion centers and the white papers produced on these topics. We have a website which is www.ahcusa.org. We certainly encourage you to get onto our website and see some of those products. Another topic of high interest that I'd like to discuss is catastrophe planning. Our focus on this topic grew out of a particular concern that our colleagues in West Virginia had about the potential of a mass evacuation from the National Capital region. It has resulted in a multi-state regional project within the All Hazards Consortium. Would one of you please comment to that?

MR. CONTESTABILE: It is a good example. Initially, West Virginia received funding to study the problem. They realized that a complete study of mass evacuation from the National Capital region should involve West Virginia, Virginia, Maryland, and D.C. This is an excellent example of the value of the All Hazards consortium. West Virginia needed to partner with some other states to solve the problem. West Virginia University, as the conduit for the funds, came to the consortium and explained, "Since evacuation traffic that might be coming our way will be coming from Maryland, Virginia and D.C. we see the need to get you involved in this study. We also see value-added from your participation because the grant requires a lot of work in a very short period of time."

The consortium was able to marshal its resources through our program management office that helps manage many of the projects we are involved in. This office had organized a number of workshops across the state of West Virginia, and they had developed notes and papers from the workshops. Probably the most notable development involved addressing West Virginia's desire to develop a situational awareness tool to monitor evacuation processes in real time. We knew that it was

unrealistic to develop that platform in the three months available for the project. We determined that we first needed to find the best breed of technologies to employ by looking first at what other jurisdictions had used. So we turned to our private sector partners and we said, "Tell us what you have done in this space. We want to bring your application experience to bear on this project." We were able to get results in a very short period of time. Mike, could you comment on that?

MR. HUGHES: Katrina caused a lot of problems for Northrop Grumman because, when it hit Louisiana and Mississippi, it devastated our shipbuilding facilities there. We are the largest shipbuilder in the U.S. and thus the storms displaced a big group of our employees. When the catastrophic planning project came to us, I had folks from the DoD side and our state and local side wanting to participate by just sharing models. . . I didn't think there was a business opportunity for us. It never even came up. We had our modelers come out and made arrangements for our engineers sit down and talk to the folks at West Virginia, West Virginia University, the other regional partners.

Because we have two major facilities over by BWI airport and out in Chantilly, Virginia, if anything happens in this region, our people would benefit from evacuating to West Virginia. So it only made sense to bring our solution providers to the table to develop a collaborative model or framework on how to go forward. We called it evacuation tooling planning at the time. It was quite successful. It was at the top of our list of things to do on the development side for corporate relations.

Discussion with the Audience

MR. CROUCH: Well, with that, ladies and gentlemen, we invite your questions for the panel.

MR. PETERSON: I am Rodney Peterson with EduCause which is a higher education IT association. I first want to thank the panel because what you have talked about today has really raised my awareness about the purpose and value of the All Hazards Consortium. I have been intrigued by your consortium for a number of years. The comments about jurisdiction versus cross-functional technology caught my attention. I think there is no denying that the regional nature of this consortium is very helpful. But I wonder what your observation is about the national effort. In other words, the national infrastructure protection plan is supposed to govern exactly what you are trying to do locally -- to bring together sector experts across functions, to share information, and to deal with all hazards. Could you comment a little bit about the All Hazards Consortium as it relates to the national process?

MR. CROUCH: Yes, and also, my response will reflect Virginia's effort. We have just unrolled a Virginia critical infrastructure protection plan. It is consistent with the goals of the national infrastructure protection plan. I am not critical of the national plan. Like many efforts of DHS, it is still in its infancy. We all have an obligation, whether it is at the federal level, local or state, to

go more than halfway in our partnership. That has certainly been Virginia's approach in working with DHS. We are comfortable with that. I think they have had terrific leadership with Bob Stephan. It takes time.

I don't see any inconsistencies there between our state effort and the national effort. From an All Hazards Consortium perspective, we are moving forward with critical infrastructure protection throughout the Mid-Atlantic region. We study the national plans but we don't just sit back and wait for direction from the federal government before we start these initiatives. Many of them are underway. Our member states have done different things in implementing critical infrastructure protection that we share. Typically, our workshops involve the practitioners who are the subject matter experts from our respective states explaining successful approaches to critical infrastructure protection, interoperability or fusion centers and how they have overcome significant challenges. Each state gives a presentation of that nature, and then there is general discussion, and out of it comes a subject matter working group that crosses sector lines. This has been true of critical infrastructure.

The NIPP probably doesn't answer all the questions. I think it is a good framework, but we have an obligation between the states to continue to share our best practices, our perceptions and provide feedback to DHS. The All Hazards Consortium serves well as a vehicle for feedback. We are in a particularly sensitive era because DHS has never experienced the transition to a new Presidential Administration in its short lifetime. I know that Secretary Chertoff and Bob Stephan and others in that Department have stated that they are committed to a seamless transition during this first Presidential transition for the Department. Part of our role at the state level and through the consortium with our academic and private sector partnerships, is to make sure that that new Administration, the new transition team, has as much input as possible on what we think has worked and what we think can be improved with the new Administration, regardless of who that is.

MR. LINDSTROM: As the host and convener for part the program for the critical infrastructure workshop, I know that there were problems that we missed. We didn't cover cyber security as much as I thought we should have. The stakeholders were not there yet. They had their hands full dealing with critical infrastructure and how to get their arms around this problem from a multiple state standpoint. They were concerned about how to fit within the federal infrastructure protection plan and how to provide feedback to Bob Stephan (who was there) about the national effort.

I noticed a growing comfort among the people who participated for the full event in sharing best practices, deciding what they could do together, and agreeing to continue the dialogue. That dialogue probably isn't going to happen at the national level with 50 states, but the regional focus works.

MR. CONTESTABLE: I appreciate your mentioning the importance of collaboration at the regional level. We believe that

the federal government has its place and has a responsibility to set out goals and provide funding and strategic direction. But all disasters are local disasters. The response is local. Even if an event escalates to a Katrina or a 9/11 catastrophe, the response never ceases to be local – though it may be necessary to bring in federal assets or out-of-state assets. There is a certain component that is a state responsibility. If the federal government is about the “what” component – what we ought to be about, what we ought to be doing -- certainly the states are about the how and the who -- how is it going to get done, the concept of operations, and which agencies and individuals will have responsibility.

This each region has particular concerns that will affect its approach. In other words, within the Gulf Coast and the Southeast region, their main concern is a hurricane type scenario and their approach revolves around that. As a result of their experience, they are a more mature in the evacuation world. The Mid Atlantic region with Richmond and Washington and New York and Philadelphia is very sensitive to terrorism. In the Upper Midwest they tend to be more concerned about tornadoes. Thus, there is a logical grouping of states that is essential to being able to react, respond and translate the federal guidance into a meaningful strategy at the regional, state, and local levels.

MR. PETERSON: Can I just quickly follow up and ask, are there other regional efforts analogous to the AHC?

MR. LINDSTROM: Yes, excellent question – one we need to address. We receive requests from many other places in the country. It is exciting for us. One of the things that we struggle with is when people call and ask if they can join us. We have had requests from people in Florida and Texas. We recognize that AHC is an important model and we hope that others will implement it. Because of what John just explained about the regional groupings, there are some very logical ways that we would like to see others do this.

MR. CROUCH: We are aware that there is a Great Lakes regional organization in the Midwest.

MR. CONTESTABLE: And Ian is here from the Southeast region consortium. We almost adopted him.

MR. CROUCH: We have adopted him. There is also a consortium in the Pacific Northwest. And I know there are discussions in the Gulf region about trying to organize something similar to our Mid Atlantic consortium. Additionally, at our critical infrastructure workshop at Penn State, we had participants from Tennessee, Ohio, South Carolina, and other states that are not actually part of our consortium. We have had a debate over the last year concerning our geographical make-up. Should any state be allowed to participate? Or should we narrow the definition? We have concluded that, while we will certainly always be happy to share information with other states, we should keep our consortium with the original nine -- which includes D.C. Our rationale is simply to keep us from getting spread so thin that we are not productive.

MR. PERLMAN: I am Lou Perlman with the Risk Analysis Center. Mr. Crouch and others have mentioned funding a number of times including grants and applications. How do you distinguish between activity and productivity and account for the value of results achieved compared to the costs?

MR. CROUCH: This is a very good question.

MR. HUGHES: From a corporate perspective, we measure our marketing communications efforts. We rank the opportunities where we spend our investment dollars based on the meaningfulness of the events.

“Meaningfulness of the events” relates to the level of intensity of the stakeholders and decision makers and the overall commitment to achieving useful results. All Hazards Forum events rank very high in this regard compared to conferences and trade shows. We are not interested in handing out pins and giveaways. We want to sit down and listen to the customer to learn what keeps them up at night. It is a qualitative issue versus a quantitative result, so to speak. We are trying to improve customer service and business relationships long term, not for short term gain.

MR. CROUCH: It is important for us to know what our colleagues are doing in other states in each of these sectors. We can serve our citizens better by knowing what they do well. It is far more effective to have a vehicle like the All Hazards Consortium to put these sessions together -- to serve as the organizing agent for us collectively --to have it done piecemeal. We are seeing efficiency with this approach in every process we undertake.

For example, in developing our Virginia critical infrastructure plan, we not only incorporated the NIP guidance, but from our participation in All Hazards, Mike McCallister in my office, contacted his counterparts in New York and Pennsylvania to incorporate provisions that he had heard about at the critical infrastructure workshop. I don’t know how, particularly across the spectrum of issues that we are dealing with, like fusion centers interoperability, and critical infrastructure protection, we could have a better network to do that.

MR. PERLMAN: If I can follow up, you all know very well the GAO inspector generals have issued several reports on DHS for over the last five years. The Department of Homeland Security has expended hundreds of billions of dollars of taxpayers’ money. Every one of these GAO reports indicates we have no measure of effectiveness, no sign that the country is any safer or better for the expenditure of this money. At the regional level, collaborative level, public-private partnerships, you have described activities, but not the value of the results. I’m not blaming you. I’m just saying this is part of a general pattern that the overseers in the Congress and its executives have found again and again. You apparently are experiencing the same thing.

MR. CROUCH: I disagree. You can be critical of DHS as the party measuring results, but one thing we haven’t mentioned is

that the All Hazards Consortium grew out of the conference at VMI that Virginia hosted a number of years ago. John mentioned this earlier. But AHC also resulted from the Maryland, the Virginia and D.C. partners here within the National Capital region, that work collectively together on a frequent basis, recognizing the importance of collaboration. It was a group called the Senior Policy Group in the NCR that was the real motivating factor.

Interoperability, as an example, has been a big issue in the National Capital region. We want it to be as good as it can be. Last year DHS measured various tactical capabilities of interoperability, and the National Capital region scored at the top of every one of those categories. This success was the direct result of AHC cooperative efforts among Maryland, Virginia, D.C., and our local governments in the region and investing DHS grant funds in our interoperability efforts to collaboratively build on what the localities, the states and D.C. had already been doing. So there are ways to measure progress. We are getting measurable results. We all recognize that we can never do enough. One of the terms we like to use is the "culture of preparedness." It is not all government's responsibility -- the individual citizens must recognize their responsibilities in this culture. That is an aspect of preparedness that we hope to address with All Hazards as well.

This partnership benefits us all. Results are not always measurable. That is one of the difficulties in the preparedness arena. For example, we have developed some preparedness measurements recently for our state efforts within Virginia. But there is an innate uncertainty about them, because they are not like tax revenues or SOL scores. We don't get that type of empirical data. But we know, based on reports from our first responder community, that their collaboration is better.

Another investment we have made using DHS grant funds in Virginia is the establishment of radio caches. We have three radio caches within the National Capital region that Virginia, Maryland and D.C. have invested in. During the Stafford tornado two weeks ago, that radio cache was deployed very effectively by the first responders in the Northern Virginia region. John, we have tornadoes in Virginia, too.

So part of the benefit is the day-to-day performance improvements due to collaboration. Emergency service jobs are easier due to having the equipment they need. Frankly, I'm skeptical about the skepticism of the studies, frankly. We have accomplished much in the last five years.

PARTICIPANT: I see a recurring theme everywhere I go. There are many agencies and organizations out there that are designed to do similar things. The ASIS organization they discussed this morning, SPIN and so forth.

One of the things that I have always liked about the consortium is my ability to participate as a little guy from a small community. Without the consortium I was not able to have impact on much of anything. Yet I was able to be involved in some of the

dialogue and in the forums, and able to participate at some level. I consider this a great benefit from where I stand. Has the consortium ever been thought about as a feeder tool or as a collaborative tool stepping down to a deeper level, it would be very helpful to develop a vehicle for a framework within the states and maybe within the local or regional levels within the states to be able to emulate the same kinds of things you are doing here. I'm not talking about forming a sub-consortium, but developing a method by local jurisdictions can take the same steps to develop the public-private partnerships and other useful partnerships. Some of this has happened on its own, but I would like to see some method by which a framework could be developed as a vehicle for local people to do the same thing.

MR. LINDSTROM: That is a big challenge and a good question for us to consider. One of the advantages we have is that multiple sectors involved. From what I have observed, this is a value multiplier. This particularly important since we don't receive a lot of money or spend a lot of money. Your suggestion could also be a value multiplier at the local level. Public-private partnerships break down turf walls. Most of us have been in the business long enough to know one of the challenges is the more local you become, the more interested people are and the more they feel the direct impact of their own territory: how responsive they appear to be, and whether they get credit for doing something good. Within the AHC, we operate way outside our home turf, so we can be collaborative and not worry about who is getting the credit. It doesn't matter. I think the closer you get to home, there is a territory dynamic there that I have observed over the years that might make that more challenging. But I'd say it's worth a try. We know there are problems at the local level. There is not a lot of cross collaboration, and there are a lot of columnar meetings. Police, fire and EMS people don't tend to talk to each other with the emergency manager in the middle trying to keep them all together. In many cases, service providers don't know each other. So I understand the question.

MR. CROUCH: Within Virginia over the past two years, we have created seven regional preparedness advisory committees. In many ways we have used the AHC as the model for these efforts within Virginia. We have the usual folks we would have from the core of law enforcement and first responder community, but we are also involving the private sector including the big box folks like Target and Wal-Mart. These businesses are very important to our hurricane preparedness efforts, for example. We have involved the academic community as well. We have used these regional groups to drive our grant process, and we are also using them to inform the revision of our state preparedness strategic plan. We encourage regional collaboration and although so it doesn't explicitly involve the local level, it is a step in that direction.

MR. CONTESTABILE: I want to just add one more thing. The bedrock issues that we are involved in can be expressed in two words: trust and a focus on the problem. We have had questions about growing larger regionally. We have had questions about imposing this model on different levels of government. At any

level it comes down to these two words. We have to engender trust across the disciplines and across the jurisdictions or they won't stay engaged. As the leadership of this group, in whatever we do, we must not be perceived as violating a trust of what our values are, what our tenets are and what we are trying to accomplish.

The second piece is to focus on the specific problem: the economy problem, the homeland security problem, the evacuation problem. It is not about the next opportunity for private sector A or private sector B. It is not about whether state A or state B has its way. It is about evacuation. So as long as we stay focused on the problem and we respect the trust issue among the parties, then we will be successful -- people will participate and people will engage. When we violate either of those tenets, we have problems. There have been a couple of instances where we wandered a bit and created issues. So I leave you with these two words, because they are the centerpieces of what we are trying to accomplish. In large measure these words represent a theme that cuts across all the presentations today -- focus and trust.

MR. ROGER: Chuck Roger. I'm with University of Pittsburgh Medical Center in Western Pennsylvania. I have been involved in regional organizations both in the private and not-for-profit sector. I also spent 27 years in banking with a small national institution that is here in the Capital region now, I'm happy to say. I want to offer some encouragement -- that based on my broad background; you folks are doing a great job. I have been involved in the weekly calls that are going on now within the state organizations on evacuation, and they are being very productive. So the process continues. I have just become actively involved in it, and I am very happy to report that you are doing a great job.

I have noticed moving from the financial sector to the health care-public health sector as I have in the last couple of years, that there is a wide diversity among the models for the various sectors of critical infrastructure. Banking is very top down, driven by a model that Secretary Martinez-Fonts and some others wisely created prior to 9/11. This model proved very effective through the 9/11 financial crisis that didn't happen. It works for the financial sector. The health care sector is driven from the bottom up in that every hospital is sheltering in place, very independent, and very self sustaining. So here are two very different models. The other 16 sectors are probably somewhere in between these two. DHS involvement, emphasis and funding towards individual sectors have been very different, too. My question is, have you given any thought to addressing diversity from a sector point of view between private and public?

MR. CROUCH: Let me just mention again, as we have noted before, each of these workshops and initiatives we have been facilitators as the board. Facilitators have not been sector-specific subject matter experts. So that is a question that frankly I would have to defer to our working group and our committee. I'm not sure whether they have addressed this or not. It is a great question.

MR. CONTESTABILE: I would answer it by saying we have great faith that the people who own the intra-sector problem will figure out a way. If there is one common denominator, it is that. To put it in private sector speak, "the customer is king, the customer knows best." We think that it is appropriate that the models vary across the sectors to some extent, because of the sector differences you allude to. We respect that by making sure we have the people from the sectors that own the problem under consideration in the room and listen to them carefully.

MR. CROUCH: Thank you for your question. . We will take that question and your observations to the consortium.

Ladies and gentlemen, thank you. You have been a great audience. I do want to call your attention to our website, www.ahcusa.org. We invite your research and your future participation if you so choose. Thank you.

MR. KNICKREHM: Thank you very much, Bob, and the rest of your panel.

Panel Three: National Security Telecommunications Advisory Committee

MR. KNICKREHM: Ladies and gentlemen, it is time for our third and final panel of the day. This morning's panels addressed public private partnerships at the local and regional levels. We will now consider a national level public-private partnership. I will let Jack Edwards, who is the panel moderator, introduce himself, his panel, and his topic.

DR. EDWARDS: Thank you. I suspect others will join us. Since the lunch in the outdoors was such a nice day today, we've had some folks who've escaped. There is no fence to keep people in. Based on my experience as a Texan, we have ways of making cattle do what we want them to do, but cattle prods are not very polite in this company.

What we would like to talk about today is some of the public-private partnership experience of the National Security Telecommunications Advisory Committee or NSTAC. NSTAC is a Presidential advisory committee chartered under the Federal Advisory Committee Act (FACA) and consists of up to 30 CEOs. Larry Hale, to my immediate right, will go into some of the background of the organization. Dan Hurley, to the far right, will talk at length about some of the actions that the government is undertaking in response to a recommendation that we made to the President a couple of years ago.

I will begin by telling about an NSTAC task force that I was asked to chair. I will go into that in a little detail. So that is how the panel will proceed. Hopefully we will have time for some questions and discussion at the end. Feel free to ask questions at that time.

I was pleased to hear the previous session on the Mid-Atlantic Region All Hazards Forum. The NSTAC is an advisory committee set up to address all hazards response in the telecommunications

arena. Telecommunications can be voice, video, or any kind of electronic communications at a distance. So it includes the Internet, it includes the next generation networks - all the ingredients of the future of telecommunications.

Specifically, we are looking at what we call national security and emergency preparedness. National security, of course, involves with things having to do with cyber events and cyber attacks. Emergency preparedness obviously has to do with preparation and response to various national emergencies -- hurricanes, floods, earthquakes and so on.

One of the things that we have worked on is the interdependency of telecommunications and electric power. Electric power and telecomm are fundamental to the operation of all the critical infrastructures, the 17 or 18 categories as defined by DHS. Of course, telecomm and power both depend on an adequate supply of water for cooling and food and everything else as well.

One of our members characterizes telecomm and electric power as millisecond kind of infrastructures. We know if an event happens in the power grid, within a few milliseconds the effects spread throughout a larger region. For example, in 1991 there was a problem in the telephone system that spread instantaneously and was corrected within a few hours or most of a day. So these are infrastructures that allow for the possibility of disturbances that are immediate and far reaching.

In 2003, Duane Ackerman, who at that time from Bell South, was the chairman of the NSTAC, came to me and asked me to chair a telecommunications-electric power interdependency task force. In the past we had looked at dependency. In the 1980s we looked at how electric power depends on telecommunications, specifically looking at Supervisory Control and Data Acquisition (SCADA) system events. In those days the SCADAs were protected by dial-back modems. We pointed out that that is not the world's best security approach. But it was good for the time.

Electric power has come a very long way since those days, and has really caught on to some of the security issues. The electric power industry is working very diligently to try to secure and isolate their infrastructure from attacks.

We also looked at banking dependencies on telecomm. We looked at transportation, most specifically the intercontinental trucking transportation and how they use telecommunications to do dispatching and things like that. We pointed out some of the ways they relied on telecomm that they weren't totally aware of. So a lot of our previous work was wrapped up and brought in under the critical infrastructure protection (CIP) umbrella. In a sense at NSTAC we were advanced, ahead of the curve, with respect to CIP initiative. There was a report issued in the late '80s describing what was called "the national coordinating mechanism." The report discussed the dozens and dozens of infrastructures and how they could be coordinated by a

single entity. This report was used in part in developing the CIP initiative. When Duane Ackerman came to me though, the topic was interdependency. He asked me two things. He said, "Look at the way that telecomm and electric power rely upon each other in a mutual embrace. Then consider how you would rebuild them if they were both gone for a period of time." I agreed to do that.

We began in the spring before Katrina. We were barely organized when Katrina occurred. Katrina provided an impetus for a lot of what we wanted to do. We initiated several ideas in the Katrina after action report. The main things we focused on in our first report, called People and Processes, included how the electric power world works together to develop situational analysis and how they work together with the state, local and even regional government entities to achieve access to a disaster site. There were some staff reaction implications which we suggested should be assessed. The report proved quite interesting. In the past, the NSTAC community used members from the telecomm world to do the work. But in this case, we reached out well beyond the telecommunications industry to the electric power industry. We put together a collegial group, which included members of the NSTAC community, members of the electric power community, organizations such as NERC, Edison Electric, and several of the operating companies including the Southern Electric Company. We reached into Canada and enlisted two or three of the Canadian power companies. We had representation of the Canadian government. In North America there is no distinction between Canada and the U.S. on electric power and telecomm. They are all very tightly interwoven.

So we were able to create a fairly good, collegial group. We spent a large part of our first few meetings trying to understand one another's language. When people talk about outages and where they occur and so on, there is a difference of viewpoint from the electric power to the telecomm side. We spent a lot of time in the aftermath of Katrina worrying about access issues resulting from the flood and the hurricanes knocking down access poles, telephone poles, and power poles.

What we concluded from the Katrina experience was that we needed a very, very strong situational analysis tool which could assess telecomm, electric power, and other infrastructures in cooperation with the new fusion centers to develop a single picture in real time. We recommended that that be done at the lowest possible level and then escalate to higher levels of integration if need be. We also saw the requirement for some sort of survivable communication among the various operation centers. The electric power companies and the telephone companies have very good operation centers, emergency centers, but they aren't necessarily connected with their own private, discrete or survivable comm.

One of the complaints in the telephone world is that they get the same 800 number to call as everyone else and must go through the same voice mail hell to get to somebody. We suggested

various ways to either have private emergency call numbers or even have high frequency radio at the centers for their use in coordinating and developing the picture. We discovered that some of the power companies had different priorities and rules about what systems to restore first.

So, all those things taken together were put together in a report to the President of the United States entitled "People and Processes." When Mr. Ackerman first approached me before Katrina, he wanted this report done first. I indicated, at that time, that it would probably take a couple of weeks to complete. But due to Katrina, we wanted to learn as much as possible from experience and it took us a year and a half to finish that piece.

The real question that he wanted us to address was, "What would happen if the electric power and/or telecomm were removed from service for a long period of time?" "Long" in this sense means weeks to months in a large region. I'd like to point out that the outages of concern have never happened in North America. When things have never happened, it's difficult to get a hearing on what to do about these things.

We did not focus on causes of such a long-term, large area power outage. We had trouble finding a way that the telecomm might be debilitated for long periods of time. Even in 1991 when the signal in system seven was out for a few hours, the system software was rebuilt put back together in an earlier version of the equipment. But we did know there were possible effects on the power grid, various effects, some of them a bit sensitive perhaps. Various effects could cause a power grid to be unavailable in large regions for some time. That does not mean it is totally out of service. Even in the August 2003 blackout that also happened around the time of our study, there were points of light -- the area wasn't totally dark. New York City had power here and there, and they brought in generators, so they were able to light up sections.

We developed a definition of a long term outage and investigated the issues surrounding restoring electric power and telecommunication service. The power industry had what they called "black start." They know how to bring up a grid from dead stop. We received a presentation from the Telcordia Company on their extensive experience on the telecomm side with telephone black start. They assured us that they know how to bring the telephone system up from a black start. Though, if you read these reports carefully, in the cases of telecomm you will find, "If the electric power grid fails and we run out of motor generator fuel and the batteries run down, we are dead in the water." So they must wait for the power grid to be restored. It may be out for quite some time. Problems arise because, when the power grid comes back up, communication is necessary to coordinate recovery of the telecomm system. When we asked, "Under circumstances when both systems are down, how you communicate to restore service -- how do you juggle the interdependency?" There was really no good answer to this question. We saw this as a question of national importance

and communicated this to the President of the United States. It is not a problem that any one company or any one industry or even two industries can address. It is really a national issue. We recommended that the issue deserved study and a decision on what to do about it. We presented our report to the President in the winter of 2006 and stood the task force down.

I represent Nortel on the NSTAC. The chairman of the board of Nortel is the Presidential appointee and I serve under his leadership. Simply put, he gets to meet with the President and I get to do the work. We have been following the progress on this issue. Later, you will hear from Dan Hurley about some of the things that the government is doing in preparation for possible further efforts.

At this point I will turn the microphone over to Mr. Larry Hale from the National Communications System or "NCS." Over the last twenty-five years, the National Communications Systems has served as the secretariat for the NSTAC. Someone mentioned this morning that they had thirty-odd years of experience in the telecomm field. NSTAC has been in existence for twenty-five years. I am working on my fiftieth year in the business. If anyone can beat that I'd like to meet you afterwards.

Larry Hale is very conversant in what we are doing at the NSTAC due to his strong involvement in the National Communications System. Larry has a presentation that explains how NSTAC and the NCS have worked together for many years. It has been a truly productive and delightful partnership. It has been referred to many times in the federal government as the pre-eminent federal government-industry partnership.

MR. HALE: The NSTAC is often cited as the pre-eminent example of public-private partnership. It has been a successful public-private partnership for twenty-five years. I'll tell you a little bit about that in my presentation.

Some of the slides in the presentation were written by attorneys so they are pretty dry. Don't worry -- I am not going to read them to you. But I do invite your attention to the glossy handouts and materials that are on the table outside the auditorium on your left. There is a handout that commemorates the 25th anniversary of the NSTAC. It explains the NSTAC mission. To address the point of one questions to the previous panel, I will address not only the collaboration involved in producing these reports, but the productivity that comes from the collaboration in advancing the cause of national security and emergency preparedness communication systems. Our productivity results directly from concrete actions that the NSTAC recommends to the President. Dan Hurley will discuss some of this work in his presentation.

Now I'll move to the dry slides. The NSTAC was created by executive order. It is an advisory committee to the President. Since I'm a government presenter, I am obliged to have a wiring diagram in my presentation. Here is the obligatory slide (see figure 4).

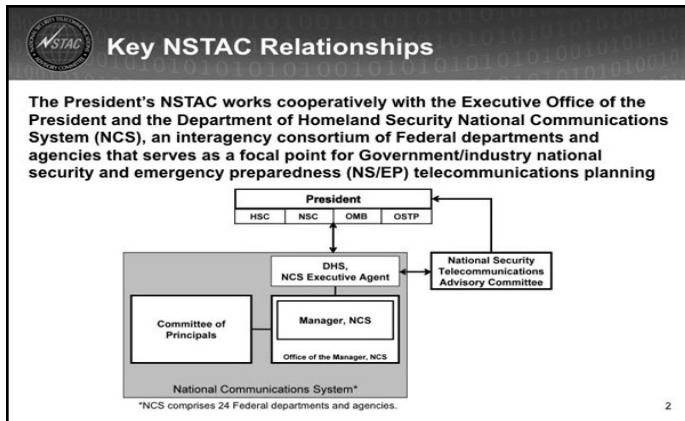


Figure 4

As you can see, the NSTAC, in the box on the right of the screen, serves the President and the Executive Office of the President represented by the four sub-blocks underneath the President. The Department of Homeland Security serves as executive agent for the NSTAC. Also, looking at the bottom of the chart, DHS serves as executive agent for the National Communications System. You will find another item on the table about the National Communications System.

The National Communications System is not a network like AUTOVON, for example. The National Communications System is a system of 24 departments and agencies in the federal government. You will see in the fine print at the bottom that there are 24 departments and agencies, each with a role in national security and emergency preparedness communications. We were formed to cooperate and collaborate to make sure that the President can speak to whomever he or she needs to under all hazards and all conditions -- no matter what the shape of the network, as long as it is there.

Regarding the NSTAC itself, by the name you might guess that the major telecommunication carriers sit on the committee. You would be correct. Representatives from the major carriers are appointed by the President to the committee. You will also notice that membership includes significant IT companies, satellite companies, equipment manufacturers, software manufacturers, and the financial sector. The CEO of Bank of America is on the NSTAC (see figure 5). So clearly the President understands that telecommunications and national security communications endeavor is more than just picking up the phone and being able to reach the governor of Louisiana during a hurricane. National security communications must ensure that the nation's economy continues to function during times of crisis and degraded communications capabilities. The President has acknowledged the fine work of the NSTAC in the 25th anniversary commemorative publication that has been mentioned.

The National Communications System supports the work of the NSTAC. The next series of slides explain how the government and the executive secretariat support the work of the industry members who are providing these recommendations to the

President. I think it is important, under the rubric of the theme of this symposium, public-private partnership, to explain the rules and roles within the NSTAC and NCS. These are important in the recipe for success. Industry and government folks must know their respective roles, and that these roles are codified. This explains why some of my slides were written by lawyers.

National Security Telecommunications Advisory Committee (NSTAC)

National Security Telecommunications Advisory Committee

- Comprises executives of communications and network services corporations
- Provides advice to the President on NS/EP communication policy
- NCS provides NSTAC with staff support and technical assistance

NSTAC CHAIR Mr. Edward Mueller, Qwest	Mr. Scott Kriens, Juniper	Mr. William Roper, VeriSign
Mr. John Stankey, AT&T	Mr. Howard Lance, Harris	Mr. Ivan Seidenberg, Verizon
NSTAC VICE CHAIR Mr. James Albaugh, Boeing	Mr. Michael Laphen, CSC	Mr. William Swanson, Raytheon
Mr. Gregory Brown, Motorola	Mr. Thomas Lynch, Tyco Electronics	Mr. Joseph Wright, Jr., Intelsat
Mr. Daniel Carroll, Jr., Telcordia	Mr. Craig McCaw, Teledisc	Mr. Mike Zafirovski, Nortel
Mr. Kenneth Dahlberg, SAIC	Mr. Walter McCormick, Jr., USTelecom	
Mr. Arthur Johnson, Lockheed Martin	Mr. Kyle McSparrow, NCTA	
Mr. Clayton Jones, Rockwell Collins	Mr. Craig Mundie, Microsoft	
	Mr. Donald Obert, Bank of America	

Figure 5

The NCS has a history going back to the Cuban missile crisis. As we learned from the previous panel, the Department of Homeland Security is five years old. The NCS has been in existence 45 years this year. Prior to the formation of the Department of Homeland Security in 2003, the National Communications System was under the executive agency of the Department of Defense. So we have a strong DoD genetic in our makeup. Our executive agent is now the DHS.

National Coordinating Center for Telecommunications (NCC)

One of the NSTAC's first recommendations to the President was the creation of the NCC:

- Created in 1984
- Mission: to initiate, coordinate, restore, and reconstitute NS/EP telecommunications services or facilities under all conditions of crisis or emergency and to assume the role of the Telecommunications Information Sharing and Analysis Center (Telecom ISAC)
- Coordinates with the Federal entities such as the Federal Emergency Management Agency, Federal Communications Commission, Department of Defense, and General Services Administration in disaster relief efforts

Figure 6

The NCC is an operational example of public-private partnership. It resides at the National Communications System. The National Coordinating Center is our situational awareness center -- our operations center, if you will. Also, as you can see on the second bullet, it serves as the communications "ISAC," the information sharing and analysis center for the communications infrastructure sector.

The NCC was created as a direct result of recommendations of the NSTAC. It continues to function today on a 24/7 watch. It

is unusual in that this is a government operations center with fulltime industry residence within the operations center providing insight back to the owners and operators of the communications infrastructure. During an event affecting the communications infrastructure, the NCC enables us to get ground truth. We can see CNN.

Here is an example that Brian Carney, the manager of the NCC, likes to use. At one of the morning briefings, DHS was concerned because CNN was reporting that communications were out in Hawaii after an earthquake. CNN was broadcasting a lot of gloom and doom. Brian was able to turn to the resident reps in the room and have them check back with their operations centers. The operations centers were able to check the status of the networks and determine that there was a brief outage after the earthquake, that the systems were coming back up, and by the time we had the briefing, that most systems were back up to full capability. So we were able to get ground truth, as opposed to depending upon questionable media reports to give us our situational awareness. We were able to do that simply because our industry members have access to their company networks and their company operations centers. For the benefit of any lawyers present, the industry members are employees of their companies. We provide them a desk and a place to plug in their computer and use the phone. For that we get their expertise and their reach-back to their company. It is a valuable operational example of public-private partnership.

Another great example of a public-private partnership in the context of NSTAC is called the NSIE, the Network Security Information Exchange. Jack Edwards, on my left, is an active participant in the NSIE. The NSIE was created to examine issues of network security. It became clear that a lot of different companies and government agencies were wrestling with the same issues. We needed a collective group to share our successes and failures and come up with common solutions. A unique feature of the NSIE is that all the participants are covered by a strict nondisclosure agreement. If you don't sign the NDA, you don't get into the meeting. Secondly, NSIE is a self-policing information sharing exchange. If you come to the meeting, you are expected to share since the information you share is protected by the NDA. There are a number of different levels of information. I don't want to get into too much detail; one level is shared information that doesn't leave that room. Participants are under an obligation to comply. You can also share information that members can freely take back to their own company, but not attribute it to the company or the entity that shared it. And there is another level of sharing that is totally open. If a member comes to the meetings and doesn't share anything they aren't invited back. They literally go around the table during the one or two day meetings.

Jack has been to a lot of these meetings. I have been to a couple of them. The NSIE just held their 100th meeting last month. They have six meetings per year – about every other month. A credit to the success of the NSIE is the fact that the U.K. and Canada

have made visits to study our NSIE experience. In fact, they invited the NSIE over to London. U.K. and Canada now emulate what we do and have established their own NSIEs. In fact, in a couple of weeks we will hold a trilateral meeting with all three NSIEs meeting together in Bath, Canada to share information among our three countries. So the NSIE is another fine example of public-private partnership that we like to point to.

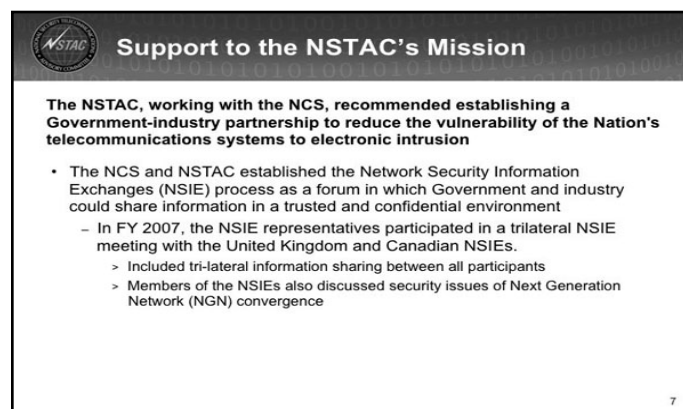


Figure 7

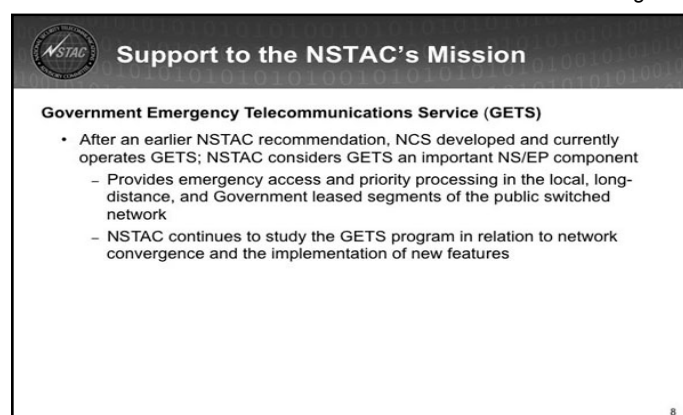


Figure 8

Now, these next slides I will whip through quickly. This is an example of the concrete results of NSTAC recommendations (see figures 7 & 8). Think of the Mother's Day effect on the old phone system back before the days of deregulation. You couldn't get through. You couldn't make a phone call on Mother's Day because everyone else is also trying to call their Mom. The same effect can occur during a crisis. In such situations, government responders need a way to get through. So the NSTAC came up with the concept of a calling card with a special code that gives government responders' calls special handling -- special routing priority. This capability was not simple to achieve. This is why we have groups of smart people like the NSTAC. Implementing the capability required an FCC rule and order to establish priority call handling. Prior to this, the FCC rules prohibited priority handling for any user. With FCC rule changes, selected emergency responders now have a simple calling card that they can carry in their pocket with a code that enables their calls to go through on a priority basis.

This wireless information service is essentially taking the same idea and translating it to cell phones (see figure 9). The wireless information service gets you the first available contact with the cell tower, so you are not blocked out of the tower. And your call obviously goes through the telephone system so you use your GETS to make sure you get through the other end.

Support to the NSTAC's Mission

Wireless Priority Service (WPS)

- Supported by an NSTAC recommendation and its own research, the NCS received authority to execute a WPS program on behalf of the Executive Office of the President
 - Program dramatically improves wireless (cell phone) components of calls and raises completion percentages
 - In conjunction with GETS, WPS raises end-to-end call completion rates for wireless calls

Figure 9

TSP or "telecommunications service priority" system is a forward thinking capability that may be thought of as an insurance policy (see figure 10). For example, if you are a public safety access point such as a 911 operating center or some other critical telecommunications node, you can get your circuits designated as telecommunications service priority or TSP circuits. If there is an outage that affects your circuit, you will get priority treatment for restoration. But, you must receive the designation in advance. Don't wait until after the outage and then ask for TSP. That is why I liken it to insurance. So these are some examples of concrete actions and results that have come out of our public-private partnerships.

Relative to the NSTAC, this is one of the slides that the lawyers wrote (see figure 11). It is a committee chartered under the Federal Advisory Committee Act or FACA. Because it was established by executive order and falls under the FACA, there are certain rules about what it is and what it is not – and what the role of the private sector is and what it is not. NSTAC members are advisors to the President. They do not serve as employees of the government, but rather, serve by providing independent advice. They are appointed by the President because they are considered to have particular knowledge and expertise in their field. They are not government employees.

As Jack mentioned, the CEOs are advisors to the President. There is a lot of work involved in supporting the CEOs in this capacity. Therefore, we have the industry executives subcommittee comprised of executive subordinates for each of the NSTAC CEO members. We came to this symposium directly from a meeting of the executive subcommittee chairs group. In today's meeting, all of our task force chairs met together to discuss their progress on their specific tracks. These meetings

occur quite frequently. Almost every day we have an executive task force meeting somewhere to plan efforts and review progress.

Support to the NSTAC's Mission

Telecommunications Service Priority (TSP)

- The NCS established the TSP program to prioritize restoration of the Nation's most critical telecommunications assets when service requests overburden networks, such as during and after natural disasters.
 - Provides NS/EP users priority authorization of telecommunications services that are vital to coordinating and responding to crises
 - Serves our national security leadership; Emergency Alert System officials; public health, safety, and law enforcement agencies; and public welfare and economic officials

Figure 10

Support to the NSTAC's Mission

What is the NSTAC?

- A non-discretionary Federal advisory committee (i.e., a Government entity)
 - Established by the President pursuant to Executive Order 12382
 - Members appointed by the President
 - Administered by DHS pursuant to E.O. 12382 and 12472
- Chartered and operated under the Federal Advisory Committee Act (FACA), 5 U.S.C. App. 2
 - Covers: "any **committee**, board, commission, council, conference, panel, task force, or any similar group, **or subcommittee thereof** which is **"established or utilized** by the President, ...in the interest of obtaining advice or recommendations for the President or one or more agencies or officers of the Federal Government...." FACA § 3(2).
 - Advisory committees perform only advisory functions. President and Federal officials have sole authority to determine what, if any, actions should be taken or policies expressed in response to reports or recommendations received. FACA § 9 (b).

Figure 11

That is the executive order. This describes some of the work that they do (see figures 12 & 13). I will make these slides available for your proceedings. What does the government do? We support to this committee to enable it to provide advice to the President.


Support to the NSTAC's Mission

NSTAC Membership

- Requirements set forth in E.O. 12382
 - Not more than 30
 - Appointed by the President
 - Shall have "particular knowledge and expertise in the field of telecommunications" and
 - "[R]epresent elements of the nation's telecommunications industry"
- NSTAC members sit in "representative" capacity
 - Not "Special Government Employees"
 - Not subject to financial disclosure or conflict-of-interest rules applicable to SGEs
 - However, certain general ethics rules do apply

Figure 12

I will next highlight examples of our most recent efforts. Then I will turn the microphone over to Dan who will talk more about the government's role in taking some of the NSTAC recommendations to the next level (see figure 15). The following slides depict the task forces and associated topics that the NSTAC develops. In the interest of time I will present them quickly. The pictures are very descriptive—these slides weren't written by lawyers.



Support to the NSTAC's Mission

NSTAC Members' Representatives


- Designated by NSTAC members to facilitate their Committee work
- Not Government officials, Special Government Employees, or Representatives
- Are not NSTAC members or alternates—may not vote for a member
- Collectively form an NSTAC subcommittee of private sector experts

Industry Executives Subcommittee (IES)

- "...[T]he Committee may establish...subcommittees or working groups composed, in whole or in part, of individuals who are not members of the Committee." E.O. 12382 § 1 (c)
- Wears the cloak of NSTAC's Government personality
- The IES—and any component subgroup—can be subject to applicable FACA rules and Government direction—e.g., holding open meetings that are announced to the public if it should perform the deliberative work of a committee product (FACA applies to entities "utilized by" Government; committees must exercise independent judgment, not "rubber stamp" IES work)

13

Figure 13




Support to the NSTAC's Mission

Key Government Roles

- Government officials:
 - work with the Committee to set/prioritize the work agenda
 - "provide the Committee such information with respect to national security telecommunications matters as it may require for the purpose of carrying out its functions." E.O. 12382
 - do not participate in deliberations
 - provide legal and ethics advice on advisory committee and NSTAC topics
 - determine whether a meeting may be closed
 - determine when NSTAC activity is subject to FACA
 - implement recommendations when adopted by the President


16

Figure 14



Emergency Communications and Interoperability Task Force

- Remained active to receive and consider feedback on the *NSTAC Report on Emergency Communications and Interoperability*
- Reviewed and assessed Government actions taken or pending related to the *Report*, including:
 - Release of the Public Safety and Interoperable Communications Grant Program
 - National security and emergency preparedness (NS/EP) priority program enhancements
 - Development of the National Response Framework
 - Creation of the Office of Emergency Communications
 - Development of a National Emergency Communications
- Determined that, at this time, no additional NSTAC work in the area is needed




18

Figure 15


Emergency communications interoperability is an area of strong involvement.

The NSTAC GPS working group basically looks at our dependency on GPS and whether or not and to what extent the communications infrastructure and other critical infrastructures are dependent on GPS for various capabilities such as the timing signal (see figure 16).



Global Positioning System Working Group


- Established to investigate the implications of a loss or disruption of the global positioning system (GPS) and how it would impact the commercial communications industry
- Examined GPS vulnerabilities and distributed an information request to telecommunications industry representatives on their use of GPS technology
- Completed and received Principal approval on the *NSTAC Report to the President on Commercial Communications' Reliance on the Global Positioning System*, which discusses the commercial communications industry's use of GPS; the impact of loss or disruption of GPS; and mitigation strategies upon GPS loss or disruption



19


Figure 16

The International Task Force looks at our own dependence on international communications as well as international connectivity (see figure 17).




International Task Force

- Continued to examine current international incident management and operational protocols and the policy frameworks related to the use of NS/EP services over the global communications infrastructure
- Reviewed international network infrastructure incident response policies and legal frameworks related to how U.S. infrastructure operators interact with foreign governments and foreign operators
- Developed an inventory of framework instruments to better describe the current policy environment
- Completed and received Principal approval on the *NSTAC Report on International Communications*, which provided recommendations to the President on enhancing global communications infrastructure resiliency, based on NS/EP communications' evolving dependence on and interdependence with global infrastructures



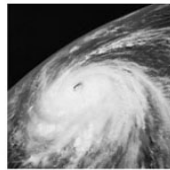
20

Figure 17



National Coordinating Center Task Force

- Remained active as a feedback mechanism on the National Coordinating Center (NCC)
- Scoped potential issues related to the NCC, including:
 - Operational consolidation of the information technology and communications sectors
 - The rewrite of the National Response Plan
 - The Emergency Support Function #2 Annex
 - NCC communications and outreach
- Completed and delivered to the Principals the *National Coordinating Center Task Force Status Report on the National Coordinating Center Roadmap for the Future*, which provided status on the recommendations and roadmap actions identified in the *NSTAC Report on the National Coordinating Center*

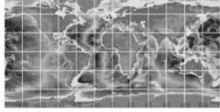


21

Figure 18

**NSTAC Ongoing Initiatives:
Global Infrastructure Resiliency Task Force**

- Established as a continuation of the previous Global Infrastructure Resiliency Working Group to:
 - Examine the potential threats posed by offshore network operations centers (NOC) in response to a Department of Defense (DOD) request
 - Evaluate NS/EP concerns associated with Internet protocol (IP) traffic management during a network event
- Completed and received Principal approval on the *NSTAC Report on Network Operations Centers*, which found that service providers recognize the risks to NOCs and have implemented steps to reduce and mitigate those risks
- Initiated an examination of traffic management during the IP evolution and potential impacts to NS/EP communications traffic during a major network event




22

Figure 19

There is always legislation on the Hill about communications, IT, etc. The Legislative and Regulatory Task Force (LRTF) helps inform each of our task forces on regulatory or legal barriers to accomplishing their goals. They also provide guidance on how to change laws if necessary. This task force is extremely important.

**NSTAC Ongoing Initiatives:
Legislative and Regulatory Task Force**

- Continued to monitor and examine legislative and regulatory activities affecting NS/EP communications, including:
 - The passage of P.L. 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007*
 - The Federal Communications Commission's Federal Register Notice soliciting information from private telecommunications carriers to help conduct a vulnerability assessment of the Nation's telecommunications infrastructure
- Conducted an examination of the 2007 cyber attacks against the Republic of Estonia to:
 - Determine if the U.S. is positioned to respond to a similar attack
 - Examine the policy considerations of defending against such an attack
- Prepared a report on the Estonia cyber attacks for Principal consideration




23

Figure 20

The Research and Development Task Force polls the research and development community and helps inform the work of all the other task forces (see figure 21).

**NSTAC Ongoing Initiatives:
Research and Development Task Force**

- Developed an NSTAC working definition of identity management
- Monitored and analyzed the development of identity management frameworks and standards in the international community
- Initiated planning activities for the 2008 Research and Development Exchange Workshop in Schaumburg, Illinois, on September 25-26, 2008, themed *Evolving National Security and Emergency Communications in a Global Era*
- Continued efforts to follow the development and implementation of emerging technologies that have the potential to impact NS/EP communications



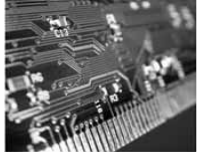
25

Figure 21

Network security is clearly a growing issue and one that we have studied with the objective of helping the government do a better job of providing network security (see figure 22).

**NSTAC Ongoing Initiatives:
Network Security Scoping Group**

- Established to scope network security concerns associated with NS/EP communications
- Met with Executive Office of the President (EOP) representatives to discuss and consider initial network security issue areas for recommended examination
- Identified a broad range of issues related to network security and focused on the following three issues for potential future NSTAC examination:
 - Core Network Security
 - Design Issues
 - End-to-End Cyber Defense



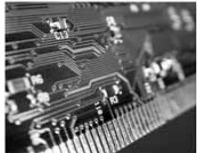
24

Figure 22

Finally, the Outreach Task Force helped me prepare my materials for this symposium (see figure 23).

**NSTAC Ongoing Initiatives:
Network Security Scoping Group**

- Established to scope network security concerns associated with NS/EP communications
- Met with Executive Office of the President (EOP) representatives to discuss and consider initial network security issue areas for recommended examination
- Identified a broad range of issues related to network security and focused on the following three issues for potential future NSTAC examination:
 - Core Network Security
 - Design Issues
 - End-to-End Cyber Defense



24

Figure 23

DR. EDWARDS: Thank you, Larry. It may have also been on his slides, but with respect to the NCC, Larry mentioned the resident members. You can guess who they might be: AT&T, Quest, Sprint, Verizon, and so on. But there are also some 35 non-resident members who don't have a physical office in the government but attend the Monday morning staff meetings and are there on call in case there is a problem. We started with the obvious carriers, but it continued to expand to include the cable industry folks. In fact, we have some representatives from organizations rather tangentially oriented to telecomm because they have an interest in the subject.

I also need to mention that there are actually two NSIEs. There is a government NSIE and an industry NSIE. They happen to meet exactly in the same place at the same time collegially. The only time they meet separately is when the industry NSIE elects a chairman. So far, they have held 100 meetings together. Within the context of these meetings there is much information exchanged that is not allowed to leave the room. There have

been cases in which a member has shared information important to the group's deliberations and then remark, "I probably would be fired if my boss knew I was telling you this." Our members include companies who are competing fiercely for business and vendors who are fiercely competing for supply contracts; but as part of the good citizenship they will share things which would be potentially hurtful if disclosed out of the room. The factoids and what happens can be shared and responses can be put together – it is a highly productive way of working together in partnership.

The main NSIE government participants are the intelligence community, the DoD community, and FCC. They also share things in a very open way. So it has been a wonderful success. I have attended almost all of the meetings and I am always amazed at how much information is shared with the group. There is a continuity of effort which fosters trust among members. If that trust were ever violated, the whole thing would come unglued. Everyone knows that. So it is strictly voluntary, strictly trust-based, and the trust has been sustained for 100 meetings.

The last thing I wanted to say before I turn it over to Dan is that we have a website, www.ncs.gov. If you go there, one of the sub-sites is the NSTAC. On our website you can find almost all of the recommendations and reports. As a FACA, the results must be publicly accessible by law, unless they are sensitive. The bulk of the reports are there. A few of the reports are not there – in particular the telecommunication-electric power industry interdependency report. If anyone here wants a copy of this report, you might try contacting Larry Hale. He can then determine whether you qualify to receive a paper copy, with the proviso that it never be posted on the Web. You must also agree not to scan it and put it in your computer. Although the report is not classified, it is sensitive.

Mr. Dan Hurley has been a longtime participant in our meetings. As Larry said, it is an industry meeting, but we do have government people attend and contribute. The final analysis though, when we vote to approve a report, the members have the final say – not the government or non-member subject matter experts. Once a report is member-approved it becomes officially an NSTAC report. Once a report approved by the principals, it becomes, in effect, a government-owned document. So the government has the right to release or not release the telecommunications-electric power interdependency report. Dan Hurley was there and was a major contributor during the entire effort. As a result, when the report went to the President and came back down for action to the Committee of Principals, Dan was given the job of leading the effort. He will now tell you about his plans.

MR. HURLEY: Thank you. Good afternoon. I would like to comment on Jack's presentation and ask a question. Jack indicated that we submitted the report to the President a couple of years ago. Well, it was more recent – December of 2006. We hope to have our follow-on response completed within two years. I simply say that lest you bond to the notion that the government operates slowly. My second comment pertains to Larry's five

references to attorneys. As a recovering attorney, I strenuously represent that remark. My question is for the audience. The screen is in the middle of the room, we are on the left side of the room, and most of you are seated on right side. Thus we are speaking to you along the hypotenuse. What might be the implication of this triangulation?

With that as a preamble, I would like to consider the "urban lore" of cooperation between industry and government. The conversation goes like this: A government representative walks up to industry and says, "Hello, I'm here from the federal government and I am here to help you." Industry people respond, "If the government would just stay out of our way we could get the job done this week." "Okay", says the government. Then, the industry reps say, "Just tell us what your priorities are, nothing more." The government says, "Okay, here is our list of priorities." The industry people look at the priorities and say, do you know how much this is going to cost? Who is going to pay for this?"

This is the archetypical urban lore on government-industry cooperation. In my presentation I will attempt to dispel this myth and by talking about some examples of government-industry cooperation from a government perspective in one small area.

The context for my remarks is the original homeland security report that came out in the spring of 2001. That report indicated that homeland security was a function of national defense and law enforcement. Anything one needed to know about homeland security could be found on the continuum between national defense – read Department of Defense, and law enforcement – read Justice Department. That was it.

We countered this notion because we contended that a major component was missing, and that was economic security. If there is any doubt about this, look at the targets in New York City on 9/11. They attempted to take out the economic and international trade hub of the United States – and they came close to making it difficult for at least a few days.

The different agencies worked in the different security components. The Commerce Department logically falls in the economic security area with other Departments as well, Treasury, Homeland Security, and Small Business Administration. That is the motivational springboard for the Commerce Department participation in a lot of the homeland security activities.

The rationale for industry-government cooperation is that industry in our country clearly owns, operates and maintains 85 percent or more of the U.S. physical infrastructure. We also recognize that industry can assist thin government staffs in identifying issues and analyzing them. An excellent example of how government benefits from industry's contributions and analysis is in the report that we have already discussed – the telecommunications and electric power interdependency report. We know from experience that, in most cases, industry participation in government activities results in better solutions

and more realistic approaches to issues, ultimately leading to buy-in and acceptance by infrastructure service providers and citizens.

Earlier, you heard Larry Hale talk about the national communications system or NCS. The NCS also has a Committee of Principals which parallels the NSTAC in some respects. Within the government there are 24 federal stakeholder agencies. The Committee of Principals received the subject NSTAC report early in 2007. This Committee established a Working Group on communications dependency on electric power at its May, 2008 meeting.

I first learned about it on the evening of July 18. I received a phone call indicating that I was to be the new chairman of the Communications Dependency on Electric Power Working Group. My initial response was, "Are you sure you have the correct phone number? This is Dan Hurley. Who are you trying to call?" I accepted the task partly because I was also informed that one of the privileges of being chair is that I could recruit my own members. I was also informed that our report was due to the Office of the President before the end of the summer in 2008. We got to work quickly.

We have as of this time 14 members from 11 federal stakeholder agencies including the chair from the National Telecommunications and Information Administration, and the vice chair from the Department of Energy's Office of Electricity Reliability. In addition, we have four volunteer participants from the private sector, including NERC, the North American Electric Reliability Council. We have had six experts who have contributed at a meeting or offline. One of the experts and presentations was Dr. Edwards, who came and briefed the working group early on about the results of the previous task force. His brief set the challenge and the charge to the working group members.

In addition to our working group members, we have five graduate interns from Johns Hopkins University, including three who had mid-level career experience in industry. We also have a very small federal support staff. Our goal is to research and report on issues relating to long term outages – not solely responding to the NSTAC report. We did not start off by strictly limiting ourselves to responding to task force recommendations. We felt that would unnecessarily truncate our research and analysis. We are taking a broader look at the issues. Before we will finish, we will make sure that our report, our findings and recommendations relate to the Telecommunications-Electric Power Interdependency (TEPI) Task Force report.

We looked carefully at how to define long term outages. It has been difficult to fathom exactly what a long term outage is because we haven't had that experience. The longest outage on record prior to Katrina was on the order of two weeks in certain areas. By "long-term outages" we mean scenarios where the power is out longer than post Katrina in New Orleans over large regions of the country. We have virtually no experience in this regime.

We organized a workshop on this subject that was held on, April 8th and 9th – just last month. We likened the event to the quest for a unicorn. Dr. Edwards agreed with this analogy and asked, "But would you like to meet a unicorn head on?" This was very apt rejoinder, and helped to crystallize our thinking for the two day workshop.

The workshop included briefings on situational awareness tools. Two of these have been used within the electric power sector. They were very helpful in sharing the tools and their related experience with representatives from the communications industry. The workshop also included a briefing on an information situational awareness tool that the communications industry shared with representatives from the electric power sector. It was very helpful to become aware of the situational awareness tools used within the respective sectors and form an opinion concerning whether specific situational awareness information is useful in the other sector.

There were 14 tasks identified which were universally supported by the working group members. We hope to complete an initial draft report encompassing all 14 tasks by the end of June 2009. We will then vet the report and submit it to the Committee of Principals by the end of August.

I haven't said much about the substantive findings of the working group and that has been intentional. Because we have not formally adopted and approved findings, it would be premature to present these. The experts represented among the working group members include the Department of Energy's expert on photovoltaic systems, fuel cells, wind power, and a specialist from the Department of Homeland Security's Science and Technology Directorate on recovery transformers. Suffice it to say, our communications industry representatives have learned tremendously from the electric power sector contingency. We hope that that the benefit has been reciprocal – that our electric power sector colleagues have learned much from their communications industry compatriots.

Our working group has involved an extensive literature research and cross sectoral discussions during the meetings. We have tried, in the interest of mercy to the working group members, to maintain the ratio of two conference calls per face-to-face meeting to guarantee and honor their support and participation.

We have learned many lessons (see figure 24). The economic security concern is a motivating factor for both industry and government. If we don't have the wherewithal to keep our economy functioning, we cannot address the national defense and law enforcement component. If we don't have the economic security component functioning, industry is not going to be able to function. We also need to have people in place to service our needs as consumers and to help keep society functioning in an orderly manner. Economic security is the motivating factor in its many manifestations.

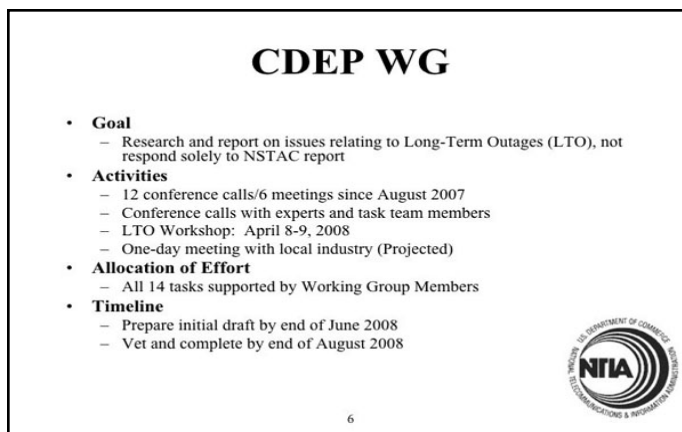


Figure 24

I've mentioned that our work complements law enforcement and national security objectives. It also complements the green initiatives and environmental initiatives such as return on investment associated with energy self-generation and energy conservation. These are some of the issues that are addressed in the current draft of the working group report.

Finally, we find that industry interaction is essential to identify the most important issues. It broadens the analytic support that is available to government organizations and facilitates the reality check. This may be more obvious in rulemaking where the government goes out for notice and comment on proposed rules. But even in working groups such as the ones that Dr. Edwards and I have led, an industry reality check has helped very much throughout our discussions. It produces tangible results – not only reports, but also tools that are used. Finally, industry interaction helps to accelerate the economic security benefits.

Discussion with the Audience

DR. EDWARDS: Before we do that, I want to make further comment on what has happened as a result of those recommendations. Nobody likes to make a recommendation and have nothing happen. The most obvious result, right now, is Dan Hurley's CDIP working group. Its existence is a direct result. There are other important results that I will not go into now because they were mentioned in Larry Hale's comments. The follow-through response to the reports is the responsibility of the manager of NCS, Mr. Jamison. He takes that seriously. He works with his staff as well as with the NSTAC members to track what has happened to the various recommendations we have made over the years.

Finally, going back to the Telecommunications-Electric Power Interdependency Task Force, we picked that as an example because of the connection with Mr. Hurley and his work. There are others that we could have picked. This is perhaps the most appropriate one to address because it is near and dear to everybody's heart and relates to the theme of this symposium. It is also concrete work we can report on and discuss.

One of the questions from the last session was, "How do we account for success, and how do we measure success?" Return on investment is high within NSTAC since the NSTAC work is pro bono. Member companies do all their work with no government assistance. The only government assistance, as Larry indicated, was NCS work. In this case there is a small contract with a government contractor who provides the secretarial work and a little bit of research. The net result, any way you measure it, is that the return on government investment is very, very high.

There are a few programs that have resulted in contracts. The Wireless Priority Service (WPS) contract was won by a company, and they did some work. But that came about because of a recommendation from the NSTAC, not because of the work we did. These were monies that were well spent, I believe.

There is also a program called NETS, which was a predecessor of GETS. NETS was the Nationwide Emergency Telecommunications System. Partly as a result of the NSTAC critique, that work was not completed and GETS was put in its place. So some of the work that we do is related to cost avoidance. NETS was a very, very expensive piece of work, had we followed through with it. As a result of some of the NSTAC task force results we suggested that the government go a different way, and they took our advice.

So measuring success is rather easy in terms of return on investment. The cost to the government is practically nothing. There is a meeting every year where we take an hour of the President's time and a day of several senior government officials. We count that hourly rate. That is the cost to the government, in addition to the support work. Our work involves a very modest expenditure on the part of the government and a relatively modest expenditure on the part of industry. The return has been that we have come up with some very helpful and in some cases profound recommendations and results.

At this point, I'd like to thank Larry and Dan. Since we have some time, I'll now open up to questions.

DR. O'NEILL: I am Don O'Neill, Center for National Software Studies. On this issue of economic security, I am interested in learning what is the joint telecomm and electric recovery time objective that you would offer to the financial sector? I ask that question because the financial sector, in its regulations, has a footnote that states that the telecomm and electrical availability is assumed based on an industry firm assertive commitment of a four hour recovery time objective. This implies that the financial sector can be assured to opening the next day to avoid economic calamity. I would be very interested in hearing a candid response in this area.

DR. EDWARDS: Let me say first of all, the way the electric power grid has failed in the last several years is fairly brittle. The way that the telecomm system has failed in the last few years is rather soft. Telecomm has backup power; it has batteries; it has diesel

fuel and generators. So unless somebody drives planes into buildings and takes out an area as they did in 9/11, the telecomm is very resilient.

Our report was in two halves. The first half was in reaction to national disasters. A hurricane goes through an area, it crosses Florida – trees fall down, telecomm wires are broken, and power wires are broken. It creates a terrible mess which must be cleaned up; and that takes time. Everybody understands that.

A long-term outage is different and unprecedented. It will take months or more to recover from the effects, to put the infrastructure back together. We didn't talk about the economic aspects of that one. Instead, we decided to look at the resources necessary to fix the power problem because everything else depends on it. Put all your effort into restoring that. In case of a long-term outage, I have advised people that the main thing to do individually is to make sure you have access to a long and well preserved supply of turnips and water. We can live on boiled turnips for a long time.

In other words, we are talking Armageddon, almost. That is why the long term outage scenario is a bit sensitive. No guarantees, but we want to make the level best to get our systems back as quickly as we can. It is like Winston Churchill said in World War II, "We shall defend our island, whatever the cost may be. We shall fight on the beaches, we shall fight on the landing grounds, we shall fight in the fields and in the streets, we shall fight in the hills; we shall never surrender..." The normal things like telecomm are there and have been there for over 100 years. Normal outages are measured in terms of hours or days. But in a long term outage, the whole thing might be out for months.

DR. O'NEILL: My take-away here is that the use of the footnote tactic in that regulation is useful, but not fully legitimate. The use of a footnote by the financial people in their regulation that says they will be up and running in four hours, but assuming telecomm and electrical, as I am listening to you and thinking that their footnote is not fully legitimate when I take your response into account.

DR. EDWARDS: I would say it is legitimate in the five nines kind of situation. Long term outages are outliers and due to causes which I don't want to go into. Under normal operating conditions, yes, I agree that the telecomm world fails soft and recovers quickly.

DR. O'NEILL: Thank you very much.

MR. MANTO: My name is Chuck Manto from Instant Access Networks. I am president of a small company doing consulting and some manufacturing related to networks. I have a fear that I would like to be allayed and a question. I need to give you a sentence or two of background. I had the great honor in the 2000 time frame of watching Nortel class four and five switches being deployed. It is a phenomenon that most people don't appreciate unless you are with those teams of people that come

from around the country and all the coordination that goes into building up one of those and deploying it. I have also had a chance to work with local governments across the country on their 911 centers and some state agencies, and helped some federal agencies in the design or deployment of their critical infrastructure, particularly in telecommunications. Alongside that, I have been doing some work, in part because of people here who worked on the EMP Commission. The EMP Commission has done some work that gives indication that there are some scenarios where you could have long term telecommunications outages simultaneous with power outages. I have been in over 100 of the central office facilities, and based on the research that I have seen, that the information on telecommunications systems is basically open source. There are scenarios where you could have widespread damage that might take months to a year or two to repair. In the work that you have been doing in the 14 areas you outlined, have you taken a comprehensive approach to the various electromagnetic inference effects, in particular EMP scenarios that were addressed by the EMP Commission? Absent that, I have this nagging fear that there may be some other scenarios that are pretty overwhelming that could result in your unicorn scenario.

DR. EDWARDS: Let me answer it two ways. First, one of the members of the task force was an EMP commissioner. He brought that to our attention. Secondly, several years ago I was the project manager for the DMS 100 EMP test suite. During these tests, we showed that, even with the machine inside a wooden box, under the full threat, the DMS 100 switch was not damaged at all. It might have a minor hiccup but the test showed it would recover almost instantly, and in most cases didn't exhibit any problems under the simulated threat. The DMS 100 equipment was designed with the capability of being directly hit with a lightning bolt, which is pretty energetic by itself. This is not to say that there are no systems that are put in the field today that might be susceptible to EMP. In fact, some of the equipment in electric power systems, some SCADA equipment, might be susceptible. I don't want to go into that; but that is a risk which should be looked at very carefully. I should add that we encourage all vendors of telecomm equipment, as part of their proof test, to submit their product to various kinds of testing methodologies to see what the susceptibility to EMP is.

All that taken together, if I were a betting person, I might find other ways to do mischief besides the EMP. One of our members on our task force from the DOE who feels the main threat is posed by good old solar storms, with a solar injection of high energy particles trapped by the earth's magnetic field. NERC is looking into that. In fact, today and tomorrow the National Academy of Sciences is holding another seminar elsewhere in town on the effects of solar events on infrastructures.

We are looking at a large number of threats. In our task force we take these as a given. We considered the effects of EMP events, solar storms, sabotage, insider action – and other threats. We focus on how to recover, how to put the system back together

in any event. A big question is how to maintain as much electric power as possible for a long enough period to determine what is wrong with the system and put it back together. Taking all those into consideration, what should you do now to improve our future preparedness? What I'm describing is in the report. And Mr. Hurley is taking these threats seriously in his current working group. Dan or Larry, would you like to comment?

MR. HURLEY: One of the issues that we are looking at in the working group is risk management strategies. One of the tasks involves looking at risk, in the mathematical sense – causation times vulnerability times consequence yields the risk. We had an expert on the phenomenology and system effects of solar storms at the workshop. We had an EMP Commissioner attended the workshop. We are looking at the issue in terms of identifying risks and means to reduce those risks. So we are clearly addressing the issue you raise. I'm not sure our efforts will result in any novel insights, but we do have the right people involved.

DR. EDWARDS: I said earlier that we have never had a long term outage in North America. We were briefed by our Canadian colleagues who indicated that the closest example that they could think of was the ice storm in the latter part of the 20th century in Quebec. The storm also affected northern Vermont and New Hampshire. The Canadian government representative informed us that, had the event lasted another day or two, they would have run out of fuel. In that region, there were problems with lost telecomm. This is what precipitates a long term outage: the fact that you can't guarantee supplies of diesel fuel for generators. The Canadians came very close to this situation during that ice storm.

The other example that comes to mind was not in North America, but occurred in New Zealand where they lost some big power feeds. Some areas of New Zealand were out of power for a long time to the point where they had to evacuate the affected areas.

MR. PERLMAN: Mr. Hurley mentioned that these initiatives would complement what you called "green initiatives." I wonder if you could be more specific or give some concrete examples of that. I'm asking because there are some cases where green initiatives actually contradict infrastructure security efforts.

MR. HURLEY: Sure. We are looking at the possibility of developing what were called "micro grids," where an independent power source such as photovoltaic systems or some fuel cell system or wind farms are harnessed to provide steady state input to a power grid. In a disturbed state, if the national grid goes down, these micro grids powered by either photovoltaic, wind power, or in some instances out in the Western part of the country, geothermal could continue to function and provide electric power for a small grid of systems most closely associated with it. These functional microgrids could then be used to restart the national grid. This is another issue where we must consider not only the technology, but also the effects of state laws and whether they allow micro-grade capability. Some do, some do not. We don't

know what the full legal ramifications yet. But we see this as an environmentally wise approach to assuring reliable power and telecommunications. The beauty of a photovoltaic system or a fuel cell system or a wind power system is they don't use fossil fuels. The output of a fuel cell is water. By properly designing green technologies into microgrids we can develop more robust electric power for telecommunications and other infrastructures. We see this approach as contributing to environmental protection. Now the second part of your question – you indicated that you see security efforts harming the environment.

MR. PERLMAN: Well, I can offer one example if you'd like. I conducted a symposium in January for the Public Entity Risk Institute on what we call the clash between the demands for infrastructure security and infrastructure sustainability. One of the papers – which I will be glad to share with anybody who wants – it was by a group of scientists from Oak Ridge and Los Alamos National Laboratories. They presented a modeling study of the future impacts of a push to greatly increase the use of renewable energy sources in the West – chiefly wind, since that is the most abundant one. The consequence of their scenarios was that in 30 years the electric grid would actually become more vulnerable to failure.

DR. EDWARDS: I would like to see their report. We looked at the problem from the point of view of the interdependency issue and not power generation. We pointed out that the communication system is becoming much more distributed. People are relying more and more on wireless. Even the units themselves are changing. Someone mentioned that the big old central offices housing DMS 100 switches draw lots of current. Modern central offices are rather small, rather energy efficient due to the improved technology. We looked at cell sites among other things. If you power these with fuel cells using hydrogen, while the hydrogen tank doesn't degrade, batteries would. So that is perhaps one way that that the system could be made be more reliable. You didn't have to worry about the refueling it in the case of an outage. All those issues are hard to look at and not easily dealt with.

As another case in point, someone pointed out to us from the Palm Springs area that they had decided to move their water supply system power from the electric to the gas grid, running it off a fuel cell and using the electric power as backup. This was done because the latency of the gas supply is longer than the milliseconds of electric power.

The same thing could be said about other kinds of alternate energy sources that can make certain critical infrastructures a bit more reliable in terms of failing more slowly than electric power. Those are a couple of examples that we have studied, without disputing your point. This issue must be weighed very carefully. I would certainly like to see that report that you mentioned.

MR. PERLMAN: I kind of left it hanging and didn't explain why they came to that conclusion, for those who are curious. To switch to wind power in the Western region, the problem is that

where the wind blows is not where the grid goes. You have to make an enormous capital investment to extend new electrical grid connections into new places which expands the whole size and complexity of the electric power infrastructure. Ultimately, it winds up overloading the circuit breakers that have been installed to help prevent a regional blackout like that experienced in the Northeast five years ago. That the conclusion of the analysis I mentioned.

DR. EDWARDS: My cousin's son-in-law has spent the last two years building wind farms in Northeastern Colorado, where the wind does blow. His wife is a veterinarian. She is the only veterinarian for 60 square miles. But that is no big deal because there are only half a dozen people living in those 50 square miles.

So where the wind blows is often not where you want to live. The top of Mt. Washington has the best wind source in North America, but I don't believe I particularly want to live there. I agree that these issues are difficult. Often people build incentives for one reason or another, and maybe they are not the best way to go, but they seem a good idea at the time.

MR. HALE: So does this veterinarian get to patch up the birds that get injured by the rotating turbines?

DR. EDWARDS: She might, but I've got an interesting insight, by the way. She is a large animal vet, the only one within a 60 mile diameter region – quite a large area. She owns horses and she successfully uses acupuncture. I submit that that lame horse won't be affected by the placebo effect... there is something to be said for acupuncture in the Far West, anyway.

MR. HURLEY: Jack, does that work for unicorns?

DR. EDWARDS: I see we are getting far afield. I want to thank you all for some good questions. I hope you found our discussion to be helpful. Our panel members will be here afterwards if you'd like to discuss particular issues. Thank you very much for your attention.

MR. KNICKREHM: Thank you very much. This is our last break. I am as your master of ceremonies exceedingly glad to tell you that we are on time and that Assistant Secretary Martinez-Fonts is in the building. We will be hearing from him at 3:15.

Remarks by Dr. George Baker

DR. BAKER: I am George Baker, Technical Director of the Institute for Infrastructure and Information Assurance at James Madison University. We are extremely honored to have the Honorable Al Martinez-Fonts with us today. He is the Assistant Secretary of DHS' Private Sector Office. His mission is to provide our private sector with a direct line of communication to the Department of Homeland Security. Thus Secretary Martinez-Fonts is actively engaged in our symposium theme – fostering public-private partnerships. This is something that everybody has been looking forward to Mr. Martinez-Fonts works directly

with individual companies and trade associations to foster public-private policy dialogue and partnerships. He has a distinguished career both in government and the private sector. His private industry experience is in the banking sector. Before coming to the Department of Homeland Security, he was chairman and CEO of J.P. Morgan Chase Bank in El Paso, Texas. Previously, he gained much international experience by managing offices in the Philippines, Mexico City, Argentina, Chile, Uruguay, Paraguay and Bolivia for the Chemical Bank. He has had much public service experience, having served on the Greater El Paso Chamber Foundation and president of the San Antonio Chamber of Commerce. He has been on Hispanic Latino advisory boards, the University of Texas Development Board, Fannie Mae Advisory Board, American Bank Advisory Board and President of the American Chamber of Commerce in Mexico City.

Throughout today's presentations, we have heard concerns about the financial sector. Because of his extensive banking experience, we are very, very fortunate to have Secretary Martinez-Fonts in his position at DHS. He has degrees in political science from Villanova and an MBA from Long Island University. We greatly appreciate getting the Department of Homeland Security perspective today, especially so, since we have an Assistant Secretary with us today as our symposium keynote speaker. Please join me in welcoming Assistant Secretary Al Martinez-Fonts to the podium.

Remarks by Secretary Alfonzo Martinez-Fonts

SEC. MARTINEZ-FONTS: George, thank you very much, and good afternoon. I think this is the really diehard group here, staying until after three o'clock to listen to my presentation. I want to thank Dr. Baker for the invitation. And my thanks to the National Academies of Science and James Madison University for the tremendous work that they have done. We have been very good partners with them over the years, and we very much appreciate the work that you do in putting on symposia like this and helping us at DHS to get the word out.

I talk about getting the word out because this morning at the American Bankers Association with a group of bankers from one of our 50 states – I won't tell you which state they were from. I was really shocked to see how little they knew about sector coordinating councils and ISACS and some important preparedness measures.

One of our biggest challenges, which I would like you to keep in the back of your mind, is, as we talk about all the things that we are doing, we generally tend to interact with a fairly small group of people – in other words, we talk to each other. One of the things that I learned at J.P. Morgan-Chase, because it was a large bank, was how to serve a large customer base. At Morgan-Chase, we had one out of ten Americans as our customer. Now every American is my customer, and it is my job to figure out how we get going forward.

Today, I will talk a little bit about the Private Sector Office (see figure 25). Many of you who have heard me speak have probably seen this slide... I use it a lot and some of you may have seen it before. It does a good job of putting my message into perspective. The 2002 law that created the Department of Homeland Security gave my office seven tasks to do, seven things to achieve. Subsequent laws over the last five plus years gave us four more things, so we are charged with 11 different tasks. I can never remember 11 things, and they don't all fit well on one slide. So this afternoon I'll cover four tasks that I believe are good representatives of the entire list.

First and foremost, my office is an advocate for the private sector. If you are in the private sector, I'm likely main guy you want to know in the Department. A lot of people say that I'm trying to sell a product. I don't have a budget. I don't buy things. I'm not on the procurement side. But we advocate clearly on strategic issues. We work a lot at getting people, goods, and trade, in and out of the country. We work on issues associated with very broad-ranging problems including real ID or the Western Hemisphere travel initiative. There are hundreds and hundreds of issues that we address that affect the private sector. We are the advocate for the private sector within DHS. We present the views of the private sector to the DHS Secretary.



Figure 25

The second thing that we do is to share information and best practices. I don't generate the information. Charlie Allen at Intelligence and Analysis generates much of the information. Our role is to make sure that we can translate that information, in an unclassified, actionable form, to enable it to be shared with more people on the front lines. We are concerned about identifying and sharing information that is important to the private sector – information that many of you need to know.

I think that there are a lot of people who believe, if you really press them, that they should be sitting with the President every morning when he gets his intelligence brief. Guess what? I've never been there myself – and there's not much chance that they are going to be invited. What you really need, as the business community, is not the classified sources and methods

that the government protects. What you really need to know as businesses is information that is actionable, that affects what you need to do. Do I need to put some guards on the back gate? Do I need to upgrade the HVAC system? Do I need to stop a truck from coming into my facility? We are doing our best to provide such information.

We are also heavily involved in developing best practices. As one example, we have done an incredible amount of work on pandemic influenza. I had the opportunity to work with Secretary Leavitt of the Department Health and Human Services and discuss needs in this area. Secretary Leavitt is worried about the sick and the dying in the event of a pandemic. He wants to make sure we have needed materials such as vaccines, antiviral drugs, and respirators at our hospitals. We want to make sure that hospitals have the necessary electricity, water, food, and transportation services, to make sure, for example, trucks are available to deliver medications where needed. We want to make sure that needed critical infrastructure is working.

With regard to pandemics, we talk to a lot of people about best practices. Because everyone here went through first grade, you all know some best practices for a pandemic. Tell me. Wash your hands. Cover your cough. Ensure social distance – stand far enough away so another person doesn't cough on you. One way to solve that problem is of course by telecommuting. So everybody is going to stay home and you are all going to telecommute. This is not so practical if you are running a General Motors plant and you are trying to assemble an automobile. But a lot of businesses can telecommute.

At my meeting with Secretary Leavitt, an insurance company in Boston asked an interesting question. They raised their hand and asked the audience, a pretty good-sized group of company representatives, "How many of you have ever asked your employees what kind of computers they have at home and how they connect to the Internet?" They explained that they had found that 22 percent of their people have 386 or 486 chips in their computer, and 50 percent of them used dialup. We are not going to get a whole lot of work done if that is the way the computer technology they use. So that type of survey becomes a best practice. By the way, it hadn't occurred to us – it occurred to someone in business who actually carried through. This is the type of interchange that we want to foster. I'll spend some time on our next task since this is what today's symposium is all about. Clearly we pride ourselves on our role in fostering public-private partnerships (see figure 26). This is not a slide that I made up just to use for this event. It is a slide I use all the time to describe what it is that we do in the Private Sector Office. Public-private partnerships are clearly the cornerstone of what we do.

Then finally, I will talk about economic consequences. I have the largest number of economists of any office in DHS – a total of seven. We look at the economic consequences from both ends – micro and macro. From a micro side, if we get containers coming in from Taiwan with sneakers and they have

a little lead seal on them that costs about 15 cents with a series of numbers, we might deem them not to be very effective or efficient. We could get one of our really smart U.S. to develop a lock RFID temperature humidity sensor with a tamper resistant global positioning system that costs \$5,000. Your sneakers from Taiwan are going to cost a lot more, and so are a lot of other things. On a micro basis we are constantly weighing the cost versus benefits of security solutions. On the macro basis, we perform most of our analysis on exercises. What is the effect on our economy if there were a 20 kiloton bomb in the port of L.A.-Long Beach? What segments get hurt and how badly? In a nutshell, that is what we do.

I want to focus a bit on public-private partnerships. This is such an important topic. Many of you may know Jan Myers. Jan is my number two guy. Jan could not get into a school like I went to – Villanova – so he went to Harvard as an undergraduate, then to MIT for a masters in chemical engineering, and finally, back to Harvard for law school.

Jan did a great paper last year on public-private partnerships that he presented at a symposium in Europe. I will just make three points from Jan's 30-page paper. It may seem a little bit simplistic here, but first you really need to have the two sides, both public and private, present. Second, you need to have a common goal to govern what you are trying to do. It is so important to see the goal in the same way. The message we just heard from NSTAC was terrific, because their goals represent not only the vision of the President, but represent the vision of industry that aligned very closely and said, we have got to work together to get this right and fix it. Then finally, you need to have a champion. There needs to be someone willing to put their neck on the line, someone who will spur progress and make sure that the work gets done.

Public-Private Partnerships

- Partnership – Two Partners. The Government and the Private Sector/NGO's.
- Common Goal – All parties have a shared and valued outcome. Win/Win.
- Champion – The leader pushing the initiative. PSO's goal is to push the business case for Homeland Security.



Figure 26

I will now share a Homeland Security example that I often use (see figure 27). It has to do with the U.S.-Mexican border port of Nogales. Arizona is on one side – Nogales, Sonora on the other side. It is one of the very busy ports on the southern border,

although not the most busy. Laredo, Otay Mesa, and El Paso are far busier. But Nogales is a place where a lot of fresh produce comes into the United States.

We were working with the folks there trying to get it moving. The Center for Domestic Preparedness or CDP, manages the ports of entry into the U.S. It has a program called CTPAT, Customs Trade Partnership Against Terrorism. The program looks at a company's supply chain and to check how their entire processes are done – in this case on the Mexican side. It could be in China; in this case it was Mexico. We address questions related to how trucks are loaded, how drivers are vetted, are the areas secure, and what kinds of security checks are performed. We trust but verify. CTPAT (Customs Trade Partnership Against Terrorism) members get a green light.

The problem that we had in Nogales was not dissimilar to what you encounter when you travel up and down I-95 on the East Coast. As you drive up I-95 you will inevitably encounter a tollbooth. As you enter Delaware there are eight toll lanes. There are three that take EZ-Pass and there are five that take cash. You went through the trouble of signing up for EZ-Pass, but there are only two EZ-pass lanes and you are stuck two miles down the road. It doesn't do EZ-Pass does you no good except for the last 100 yards.

A Real Life Example

Nogales, Arizona Port of Entry		
	Anticipated	Reality
Cost:	\$10MM	\$3.2MM
Project:	One Lane	Two Lanes
Time:	5 Years	18 Months
Source of Funding:	Federal Gov't	\$1MM Federal, \$1MM State, \$1.2MM Private Sector



Homeland Security



Figure 27

So the joke in Nogales became, "how long does it take a member of CTPAT get through the border checkpoint?" The answer was 120 minutes. The other part of the joke was, "how long does it take a non CTPAT member to get through the border checkpoint?" The answer was 121 minutes.

It was clear we needed to build better infrastructure. We went to GSA, who has been a great partner. Their projected cost was

\$10 million. They could only build one lane on the U.S. side. None of the improvement could go into Mexico – no U.S. taxpayer money into Mexico. It would take approximately five years with Presidential permits involved, et cetera. All costs would be paid by the federal government, i.e., from your pockets. We were paying for the whole thing.

When we sat down with the Board of Trade Alliance and brought together the vegetable folks, the Mexican businesses that import automotive parts, and other private companies with a vested interest, we were able to reduce that cost to \$3.2 million. Due to the public-private partnership, we managed to build two lanes, one of which went three quarters of a kilometer into Mexico because some of the money, as I will explain in a minute, came from the private sector. It took us 18 months, including the Presidential permit. In this country where we have a large deficit, \$1M of the money came from the U.S. federal government as opposed to GSA's initial \$10M estimate. Another \$1M came from the state, and \$1.2 million from the private sector.

So here is an outstanding, very tangible example of a public-private partnership exhibiting all of the characteristics I laid out earlier. I must add that it was CBP who made this happen from an operational standpoint. The implementation partnership also included our office, the State of Arizona, the government of Mexico, Mexican Customs and the City of Nogales. All of these organizations worked together. It was not automatic. We had to do a lot of pushing and shoving to get people together and make it happen.

Skeptics may say, this was a very small amount of money and a small project. But there are many other examples – four or five others that we were involved in that were much larger. The Nogales effort led to another effort called the “Twenty-five Percent Challenge in the Detroit-Windsor area. The University of Michigan has estimated that delay of trucks getting across the border coming into the United States costs our economy \$5B per year.

At the U.S.-Canada border in the Detroit-Windsor area, there are three crossings: the tunnel, the Ambassador Bridge and the Blue Water Bridge. We developed a challenge to reduce the time that it takes to get across the border by 25%. We this objective could be met either by reduce the crossing time by 25% or increasing the product throughput per day by 25%.

To make a very long story short, we spent about \$5M to meet this challenge quite successfully. Again, it was a public-private partnership. The Ambassador Bridge is owned by the private sector. The tunnel is owned by the city but operated by a private sector company. The Blue Water Bridge is owned by the counties on either side, Canadian and American. We reduced the wait times by over 55 percent. We spent \$5M that gave us a return on investment worth over \$2.5B. It was another real and successful public-private partnership yielding a very tangible return on investment. Currently, we have been working with the Border Facilitation Group on the U.S.-Mexico border to try to improve cross-border throughput.

The Critical Infrastructure Partnership Advisory Council, or CIPAC, to me is one of the all time greatest public-private partnerships (see figure 28). Bob Stephan, my colleague, and the Assistant Secretary for Infrastructure Protection, runs this. Jim Caverly of Bob's office is responsible for the care and feeding of that group.

The CIPAC partnership involves a process under which we have designated 18 critical infrastructures. For the longest time we had 17, but just recently we added an 18th critical infrastructure. Those critical infrastructures were self-organized. It was like that old Saturday Night Live routine – talk amongst yourselves. Go over there, bankers, and talk amongst yourselves. Go over there, energy people, and talk amongst yourselves. Telecommunications people – talk amongst yourselves – and so on.

CIPAC Policy Action

- DHS established the Critical Infrastructure Partnership Advisory Council (CIPAC) to operationalize the partnership structure, and chartered it to:
 - “...unify the Federal infrastructure protection programs with infrastructure protection activities of the private sector and of State, local, territorial, and tribal governments”.
- The activities of the CIPAC are exempt from the Federal Advisory Committee Act (FACA)
- The CIPAC creates this protected space for Sector and Government entities to collaborate



Figure 28

We brought the government side together and told them, “If you want to talk amongst yourselves, you need to make sure that you involve the private sector.” The important element of this slide is a four letter word – FACA, the Federal Advisory Committee Act. The Secretary of DHS used his authority to exempt this entire CIPAC group from FACA. I know it sounds like the government trying to hide things. But it is not a matter of hiding things. If we are going to publish what we discuss in these meetings in the Washington Post or the New York Times tomorrow, no one is going to talk. We needed to have a legal structure that would exempt us from FACA and allow us to have a productive relationship between the companies – and most importantly, between those companies, or that industry sector and the government. CIPAC successfully created the protective space to do that.

Here is what I was trying to draw just a minute ago (see figure 29). We have the sector coordinating councils over on the left and the government coordinating councils on the right. Many of these things are very familiar to you. Since I was a banker, I will talk a little bit about the Sector Coordinating Council (SCC) for banking and finance. We estimate that there are about 28,000 firms included in this sector. By the way, the railroad piece of the transportation sector is a little bit easier because there are only six big ones. Banks come in all sizes, shapes and colors, insurance companies, brokerage houses, et cetera, numbering in the tens of thousands.

In the agriculture and food sector, I'm not sure we have been able to count them all. If you were to take every single farm, every single food processor, every single supermarket, bodega, restaurant, corner deli that could theoretically be a member, it

would go into the 100's of thousands or millions. So our sector coordinating councils vary tremendously from sector to sector. They are not a cookie cutter. However, they are self-organized, and that is very important.

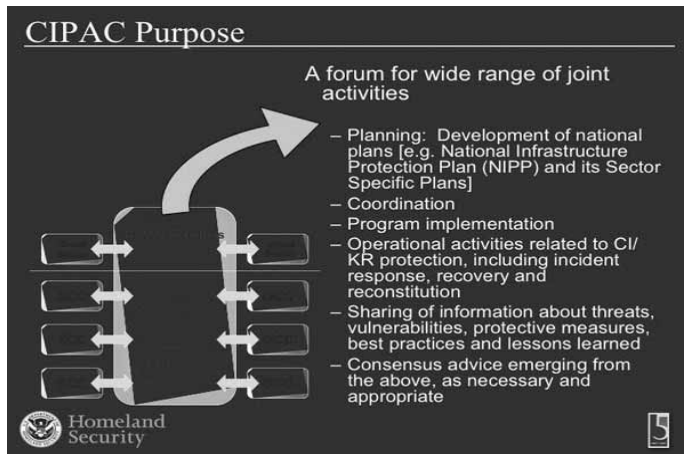


Figure 29

On the government side, we pick a lead agency. As you might guess, the Department of Treasury is the lead agency. But there are other Federal organizations that are stakeholders and involved – The Office of the Controller of the Currency (OCC), the FDIC, the Federal Reserve, and, of course, the Department of Homeland Security. We want those people to be active members of the Banking and Finance Government Coordinating Council and talking among themselves as well.

At the end of the day, this is why the FACA is so important – to enable us to draw a loop around the Sector Coordinating Council and its analogous Government Coordinating Council, so that we can have a true public-private partnership. At the same time though, don't forget that we want to draw a different loop around all of the infrastructure Sector Coordinating Councils. While you may ask what do the dams people teach the bankers? I don't know. I don't know what the bankers can teach the dams people, but there is a lot of interaction. It is very clear to me what the telecommunications folks and the electricity folks need to do in working with the bankers – because, for example, our payment system depends on the telecommunications network and our ATMs depend on the electric power grid. There are huge interdependencies among these groups. And we are still discovering interdependencies with and among the other infrastructures.

If you wrap a big bubble around all of this, you create what is known as the Critical Infrastructure Partnership Advisory Council (CIPAC). The CIPAC umbrella facilitates the partnerships needed to protect our critical infrastructure. To me, this is one of the greatest examples of a public-private partnership. While I will admit that it is not perfect, it is much better than it has ever been. We have been able to get a lot farther in achieving homeland security objectives because of the enthusiasm and the buy-in

generated by CIPAC. Within the last 12 months, we have had much success including the state and local government officials in our partnership as well.

I like to think of my office and what we do as being an inch deep and a mile wide. We cut across every single industry – the corner dry cleaner and the nuclear power plant theoretically are my customers. Bob Stephan is also helping those 18 sectors and also an inch wide and a mile deep. He can reach every single nuclear power plant in the United States, in theory every single bank, in theory every single food establishment and so on.

If you think of those up and down skinny lines, when something happens, it happens in a place. So, for example, the nuclear accident could be in Alabama, the state of Washington, or Virginia. In our contingency planning for such high consequence events, we need to be sure we are prepared by engaging the state and local partners responsible for emergency response and recovery. So if we have a nuclear accident or something we suspect to be terrorism or sabotage in Alabama we need to tell the people in Washington State or Virginia or Florida or California or wherever we suspect there could be similar activity. But isn't it just as important that we let the banks in that area and the schools in that area and the businesses in that area know?

So if you think of the grid that I am drawing up here (see figure 29), the idea would be to close these two grids so that we can have complete coverage around the country. One of the newest features that has been added to our schema is the inclusion of state and local governments to make sure that we not only go into sector specific groups, but that we work from the federal through the state to the local level.

I'm not going to read the information on the right since you all probably have been reading it as I have been talking. But I want to recognize that this is all happening.

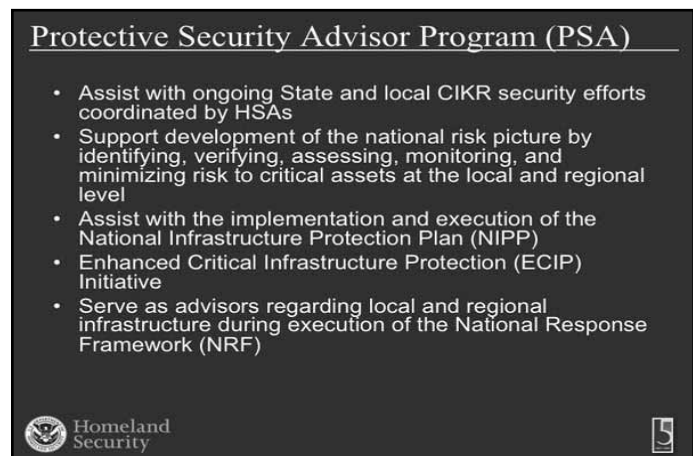


Figure 30

Let me now turn my attention to a second program that also falls under our critical infrastructure group (see figure 30). This is the Protective Services Advisory Group (PSAG). Can I just see

a show of hands – how many of you are aware of these people? They have close to 100 members now that are physically located in every one of the states and territories. They are working with the homeland security advisors in their area. They are kicking the tires of critical infrastructures and key resources to understand the risk picture. They are asking questions such as, “Where are the power plants? What are they near? What do they need to protect against? What needs to happen?” To a certain degree they are using the National Infrastructure Protection Plan (NIPP) as our bible. That is what we are all working to. This specific group has been created to address the most important, tier one and tier two facilities under what is called the enhanced critical infrastructure protection initiative. We have people all around the country making these connections, making these links, and making sure that they have had the kind of assessments that are needed.

Here are some statistics that I was provided by Bill Flynn who is DHS director of the Protective Security Coordination Division within the Office of Infrastructure Protection (see figure 31). They have made 17,420 personal contacts. If you look at the third line, we are looking at 516 site assessment visits and 2,059 buffer zone protection programs. The site assessment visits involve looking inside the fence and the Buffer Zone Protection Program looks outside the fence. The PSAG puts these two things together to look at the entire risk picture.

Problems such as anticipating the consequences of and response to a toxic release by a chemical plant are addressed. What would be would be the chemical effects and area coverage? How able is the locality to respond? Does the fire have the special equipment needed on hand or would the equipment need to be brought in?



Figure 31

This slide gives you some statistics of what it is they are doing. They conduct tabletop exercises. They work with the fusion centers in each one of those states. They provide support to the principal federal office and the federal coordinating officer in the event of an incident. The principal federal officer is for

the Secretary of the Department, the federal coordinating “very difficult” officer is FEMA. They are the guys with the money and can write checks when an event happens.

This is a public-private partnership success story (see figure 32). When the California wildfires occurred, we were able to go to the joint field office in Pasadena. We worked with the California State Emergency Operations Center (EOC), the L.A. and the San Diego EOCs. We were able to bring together the state and local governments and the private sector. At the end of the day our biggest concern was the private sector. But we couldn’t just attend to the private sector, we had to coordinate with the police and fire departments since the police and the firemen are regulating these things. We had to make sure that the action was totally integrated across all responding organizations.

I am a huge believer in the value added by all of us working together. You heard my bio. I spent 30 years in the private sector. People felt that, since I worked with the government quite well, I must be comfortable working with government officers. The truth was that every time the government called me up I hated it. I feared that they would probably demand something, ask me to do something, or request that I spend some money.

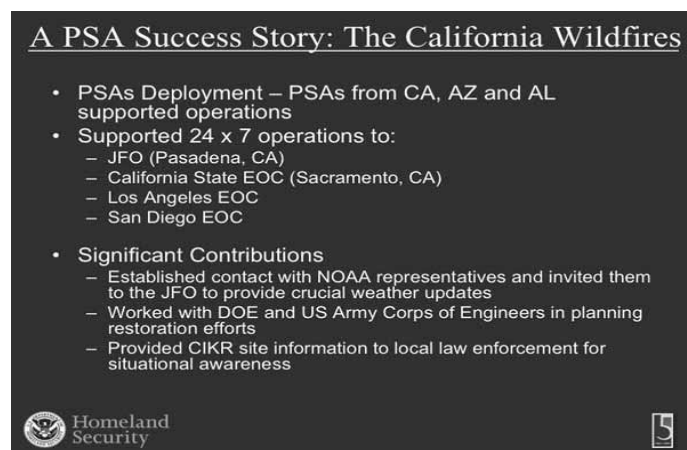


Figure 32

Now that I am in the government, I talk to career government people who believe that people from the private sector are just pushing a product or trying to sell you something to get your dollars. I’ve learned from experience that both examples are wrong. There are some wonderful people in the private sector who have real commitment to making this country safe and secure, and there are some fabulous people in the government who understand that we need to protect the private sector and are willing to go above and beyond the call of duty.

We don’t know what the next high consequence event will be, but believe me, it is going to happen. Being able to mesh these two sides together to create public-private partnerships, I am convinced is the key to making this country stronger, to make

it more resilient, and to be able to solve the kinds of issues to prepare us for the next attack, the next hurricane, the next incident.

Discussion with the Audience

PARTICIPANT: This morning we talked about incentives in a lot of different venues and a lot of different vehicles. But are there any incentives related to the private sector to engage public folks to create these partnerships?

DR. MARTINEZ-FONTS: It is getting a little bit better, but not very good. I think I recently asked my economist to look at all of the grant money and figure out what percentage of it goes to the private sector. It is minimal. The approach has been that we will help you coordinate but that the private sector needs to take care of itself. On the other hand, DHS has awarded more and more grants. The recent interoperability grants – the billion dollars that came out of Commerce and DHS is a very good example. A lot of that money will end up in the private sector. And FEMA has a series of grant programs that do help the private sector.

We have looked at a number of things. From the very beginning we were told that tax incentives are a no-no. They are not going to happen. That is the carrot approach. We have looked at the stick. Do we add another feature to Sarbanes-Oxley, which is already a dirty word in the private sector? Do we add another requirement such as mandating assessments?

One of the things that we are working on that I think will be very helpful is something called Title 9 of the 9/11 Commission Act. Title 9 involves voluntary preparedness. I know that sounds like an oxymoron, voluntary preparedness standards might work as a carrot incentive. The concept is still being developed, but the idea is to apply existing standards to private sector preparedness. We don't want to invent new standards. We are going to use an FBA 1600, ISO 23999 standard. The idea is to ask companies to apply existing standards to certify their critical facilities. There will be several options. Companies can self certify – if you are a small company you are more than likely to do that. Companies have the option of getting a second party certification. For example, if you are an automotive supplier to one of the big three you could get them to certify you. Or, if you are one of the big three car companies you would probably get an independent audit of your preparedness.

One of the things that has happened is, CTPAT has now become an industry standard. It has not been mandated, but if you want to bid on business for a large multinational corporation, the buyers will check to see if you are CTPAT certified. If you are not, many will not consider your offer. No government mandate here. It is industry self-enforcing by acknowledging that the effort to comply with CTPAT results in a less risky product or process. General Motors doesn't want the drugs, the human smuggling or, God forbid, the nuclear weapon on its truck or container coming from Mexico. So General Motors will not hire someone who is not CTPAT certified.

So how do we look at this Good Housekeeping seal of approval under Title 9? Again, just picking names, Chrysler has six suppliers for tires. Chrysler asks each supplier if they have a resiliency plan – how are they going to continue operations under stress? For the sake of argument, four of these companies are CTPAT certified and two are not. Chrysler may choose to focus on the four certified companies and eliminate the other two from consideration. That will put pressure on the non-certified companies to take CTPAT seriously. This process will raise the bar and greatly help in making a more resilient economy and society.

PARTICIPANT: Two quick questions. The first, has the private sector office ever considered holding a symposium to feature examples of public-private partnerships such as SEERN and the Nassau County folks? Secondly, as we look toward a new Presidential transition, what are some of your thoughts about using the transition to reach out to private sector folks and allay their fears about the termination of the present administration's initiatives? Thanks again.

DR. MARTINEZ-FONTS: I appreciate the question on the transition, and I would like to talk about that.

On bringing people together, we have very aggressive in this endeavor. However, most of our initiatives have focused on relatively narrow subjects. Topics have ranged from pandemics or, after Katrina we organized the first of the "New Orleans get back on your feet" type of symposium. We had a symposium in North Carolina that was ostensibly to address pandemic preparedness but became a general preparedness event. The purpose was to help the city, the state, and local business to work together.

I appreciate your asking the question concerning the transition. I know from firsthand experience that if there is one thing that keeps the Secretary and the Deputy Secretary up at night, it is a nuclear weapon coming into the country. The other topic that keeps them up is the transition. The good news is the Secretary, in his disciplined way of doing things, has driven the transition process. About a month and a half ago, we had the opportunity to bring together the top 180 people in the Department at a special off-site planning meeting. In the past we have had about 50 or 60 political appointees going to these off-sites. Our meeting of 180 allowed us to include the next two levels of civil service people in the exercise.

I'll just tell you a quick story. The Deputy Secretary met with a small group of us at this special off-site and asked, "What do you all think about this?" I was fairly critical of the event – I said, "I think it stinks." He said, "Okay, you are in charge of it." So I was in charge of this off site. We got FEMA involved, we got Miami and we asked a Task Force out of Key West to help us put exercises together. One of the exercises was similar to TOPOFF 4 and included dirty bomb events in Seattle and Arizona. The exercise scenario centered here in Washington, D.C. on Inauguration Day next year, January 20, 2009 at four o'clock. Subsequent to the

exercise game catastrophe, the first response was, “Somebody call the Department of Homeland Security.” That begged the question, “Who is in charge of the Department of Homeland Security at four o’clock on Inauguration Day?” We probably won’t have a new Secretary, but we do have an order of succession. So we played the order of succession as a top priority. Subsequent to that meeting to consider transition issues we sent roughly 120 civil servants off again to Glencoe, Georgia, to the Flexi Center to spend three days working on other exercises. My point is that we want to make sure the transition occurs smoothly. We are aware of the fact, we saw it in Spain, and we saw it in London, in England, that during times of transition, the terrorists feel that we are most vulnerable. So that would be a time to try to strike – to catch us off-guard.

I think you asked about transitioning projects and programs. Unfortunately gets into the political side of things that are very hard to project. We don’t know what the new administration will decide to emphasize or de-emphasize. By way of encouragement, we have endeavored to make sure we have our program solidly in place and we have a cadre of people that will be able to take over without missing a beat.

MR. ROGER: Chuck Roger from the University of Pittsburgh Medical Center (UPMC) and former banker, too. I’m in the health care sector now and the past two years, and mentioned this to the All Hazards Consortium folks in the morning panel. My question is, do you think it is an opportune time across all of the sectors now to analyze the different types of relationships that we have. You mentioned before, in the finance side we have got the business and federal government folks talking to each other on both sides. It is very different in the health care sector, where we have a bottom up type of structure with resilient hospitals and so forth.

Do you think it is time to start comparing the various sectors and their practices and to identify best practices and then trying to improve some of the things we’re doing? The folks from NSTAC have a great history. I have dealt with them a long time, and they have a really good program. There is an industry buildup and progress around that. The same is true with the North American Electric Reliability Council (NERC) and the folks in the energy sector. Part of the challenge that I see as you did from the banking sector is, I can buy my own generators and I can make my own electricity, but I can’t run my own phone lines between Pittsburgh and New York. In the hospital we have different challenges with procurement and supply chain and so forth, and keeping the patients up.

DR. MARTINEZ-FONTS: That is a wonderful question and it is one we have to answer. I think what you are saying is to take all the sector coordinating councils – and they do meet under the Critical Infrastructure Partnership Advisory Council (CIPAC) group – and ask what are you doing, how are you doing, what are the best practices.

I hope nobody takes this as gospel. But there is a parable about the guy who plants his field and there are weeds coming up. Someone suggests that they should pull up the weeds. He says, don’t do it yet, let’s wait for everything to grow up and then we will pick the weeds and then separate the wheat from the chaff. At this point, to be very honest, after five years we are still in that nurturing environment. We are trying to get all of the good ideas out from anybody and everybody. It is very hard for me to admit that I don’t know everything, but I don’t. There are very few people who do. So we are trying to figure out how and which of these things work well.

I happened to mention banking because banking has worked very well. I know transportation, because of its diversity, has had a lot of issues. Food and agriculture is just so huge and so diverse. Railroads is the other extreme – it’s not nearly as difficult to corral six people in one room and those folks are very familiar with safety and security and all kinds of things.

So the answer to your question is yes, that is the ideal. That is where a lot of the best practices we talked about could be used. We just started to put something together like that to help develop best practices for fusion centers. Fusion centers are owned and operated by the states. So we put money into them and we put people into them, but they are their states’. Without going into a civics lesson, they own and operate them. So our idea was to determine the best practices for engaging the private sector by looking at what’s happening across the States – what is Arizona doing, what is New Jersey doing, what is Chicago doing and so on. The challenge was to organize a forum to bring all the States together to exchange ideas. Your suggestion is important to the future.

MR. PERLMAN: I am kind of embarrassed to follow a great question with a boring one. You mentioned that CIPAC is exempt from Federal Advisory Committee Act (FACA). What about the Freedom of Information Act (FOIA)?

DR. MARTINEZ-FONTS: I’m not a lawyer. The answer is that CIPAC would be exempted. In other words, part of the whole FACA provisions would be that those records are not “FOIA-able.” I would have to get a legal opinion on it, but you don’t have to have open meetings, you don’t have to publish your results.

Thank you all very much. I appreciate it.

Symposium Recap

MR. KNICKREHM: Our last act is a class act. We have two of the smartest people at JMU to give us a brief wrap-up. First, we will hear from Dr. Jerry Benson who is Vice Provost for Science, Technology, Engineering, Mathematics, Health, and Human Services. Finally, we’ll hear from Dr. Robert Reid, who is dean of our College of Business.

DR. BENSON: Bob and I serve as the only agenda item between now and you getting out in front of the traffic, so we will make this short and sweet.

First, on behalf of Bob and myself and everyone at James Madison University, I wanted to relay our thanks to all of the presenters and panelists today. I know I found the format to be very beneficial, in looking at the dynamics of the public-private partnership at the local, the regional and the national level. The dynamics within those levels and also as the Secretary was pointing out, the dependencies across those levels are very important to understand. We've shed some important light on these today.

I also want to bring special recognition to Secretary Marsh and Congressman Ruppertsberger, particularly since both of them have provided some historical contexts to today's discussion. That was their focus of James Madison. The fact that Madison represented and had a greater national ideal that motivated him. His work and the work of his colleagues in bringing together 13 very disparate entities to work together for that national ideal really lays the groundwork and sets the mission for what we are about and what we have been talking about today.

Madison's focus on an educated citizenry as being necessary for government, what we have heard today about, individual citizens needing to step up and not be totally dependent upon our government. Also, Madison focused on the power that comes from knowledge and how we need to communicate and share that knowledge so that we all are empowered.

From my own perspective which is in psychology, I was looking at the title today, fostering public-private partnerships. As I think of partnerships, I was impressed by the first panel this morning in which one of our panelists talked the importance of forming long-term, trusted relationships such as marriage. In psychology there is something called social exchange theory. Rather than thinking of it as a marriage, the partnerships we have been talking about today, to me are more like dating. Marriage implies some kind of longer term contracted commitment. We talked about how to get people together, how to get them to know of each other, how to determine what resources they bring to the table, how they meet each other's needs, and how some of my resources can be exchanged for their resources. Based on these considerations we can develop a relationship wherein the exchange of resources keeps us tied together, rather than some external force. Many examples have been presented today of that kind of partnership. Fostering that kind of partnership obviously means bringing the groups to the table. As the Secretary pointed out, it takes two to have a partnership. We need to bring the individuals and the groups to the table.

We have heard a lot today about the government sector and the private sector, but I want to re-emphasize the benefits of including the academic sector and its role in the process. We have talked about relationships needing to be developed based on trust and knowledge, what are the incentives to bring those

people to the table, to keep this kind of collaboration going and sustain it over a period of time. My colleague, Dr. Reid, will now speak to some of the design dynamics of that process that we have heard about today, and also what are some of the success dynamics that we have heard across these groups today. I will now turn it over to Bob.

DR. REID: Thanks, Jerry. I want to focus, as Jerry said, on design and behavioral characteristics of public-private partnerships. We started out this morning talking about the work of many heads and many hands. Here are some themes that came out of the morning discussion that were continued the rest of the day.

First, the important need to understand and appreciate the common language of the different partners that is oftentimes initially not understood. Then, there is a need to understand the problems as defined by the problem owner. We talked a lot about the necessity of mutual trust. We also talked about citizenship extending far beyond narrow interests or self interest. Related to trust, we talked a lot about honesty. We talked about direct communication, oftentimes brokered by a third party that may not have a direct interest in the discussion initially. We talked about mutual respect, patience and the communication process.

We talked about focusing on problem solutions using shared resources. There was some discussion about a culture of collaboration and the need to build it, sustain it, and cherish it – to make sure that the culture exists. Also several presenters today talked about the need for a breadth and a depth in the approach to cooperation and partnerships.

Then finally, as we got towards the end, we talked a lot about outcomes both being people-driven and process-driven. We talked about metrics for both activity and productivity. One of the best examples of the importance of and results of public-private partnerships was the first panel this morning – when we get partnerships right there is the tremendous shared group pride and dedication that we saw. It is very tangible and it is very real.

With that, we will close. Thank you for being part of this event.

Representative C.A. Dutch Ruppersberger Maryland

Congressman C.A. Dutch Ruppersberger is serving his third term in the United States House of Representatives representing the citizens of Maryland's 2nd District. Congressman Ruppersberger is known as a consensus builder who works with Members from both sides of the aisle to get results for Maryland and the nation.

The Congressman serves on the prestigious Appropriations Committee. The Appropriations Committee is responsible for funding federal budgets including agriculture, defense, energy and water, foreign operations, homeland security, the environment, labor, health and human services, military, science, and transportation. He also serves on the Commerce, Justice, Science, and Related Agencies Subcommittee, the Financial Services and General Government Subcommittee, and the Legislative Branch Subcommittee.

In what Congressional Quarterly called "a coup", Congressman Ruppersberger was the first Democratic freshman ever to be appointed to the powerful House Select Committee on Intelligence. The committee oversees the collection and analysis of intelligence information from all around the world to ensure our national security and prevent potential crisis situations - especially terrorist activity. The Congressman is Chairman of the Technical and Tactical Intelligence Subcommittee. He also serves on the Terrorism, Human Intelligence, Analysis, and Counterintelligence Subcommittee and the Oversight and Investigations Subcommittee. Congressman Ruppersberger was hand-picked by the Democratic Leadership and named an Assistant Whip. In this prestigious position he meets regularly with the House leadership to help set legislative priorities and to ensure the passage of key measures.

Creating jobs and improving the Maryland economy is one of Congressman Ruppersberger's top priorities. He is working hard to provide high-quality, affordable healthcare for everyone and help seniors purchase reasonably priced prescription drugs. The Congressman is also fighting to keep our country safe and get our first responders the funds they need to protect our communities and our families.

Maryland's 2nd District includes parts of Baltimore City, Baltimore County, Anne Arundel County and Harford County. It is a vital center of trade and commerce for the state and national economy and includes Baltimore-Washington International Airport, the Port of Baltimore and thousands of businesses and manufacturing concerns dependent on these international gateways. The 2nd is also home to the National Security Agency, Fort Meade, Aberdeen Proving Grounds, the Coast Guard Yard at Curtis Bay and other installations essential to the country's national security.

With more than 20 years of public service experience, Congressman Ruppersberger has spent more than two decades helping his community as an elected official. Before being elected to Congress, he was the Baltimore County Executive from 1994 to 2002. Under his leadership, Baltimore County was named one of the nation's four best-managed counties by Governing Magazine in 2001 and is still one of only 19 counties nationally which continue to receive a triple-A bond rating from all three of the country's bond rating agencies. Prior to serving as County Executive, Congressman Ruppersberger served nine years on the Baltimore County Council and was twice elected as Council Chairman.

The Congressman chose a political career after a near-fatal car accident in 1975 while investigating a drug trafficking case as a State's Attorney. With luck and the dedication of doctors at the University of Maryland's renowned Shock Trauma center, he survived. After recovering the young investigative prosecutor decided to run for public office to help others and to repay Shock Trauma for saving his life. Today, he remains an active supporter of the hospital, serving as Vice Chairman of Shock Trauma's Board of Visitors.

A native of Baltimore City, Congressman Ruppersberger spent his summers as a lifeguard in Ocean City. He attended Baltimore City College and the University of Maryland at College Park, where he played varsity lacrosse. He earned his Juris Doctorate from the University of Baltimore Law School.

The Congressman has been married for 37 years to his high school sweetheart, the former Kay Murphy. Together they have two grown children, Cory and Jill.



Presenter Bios

Alfonso “Al” Martinez-Fonts, Jr. Assistant Secretary for the Private Sector Office Department of Homeland Security



On November 27, 2005, Alfonso “Al” Martinez-Fonts, Jr. was appointed Assistant Secretary for the Private Sector Office at the Department of Homeland Security. For the previous two years, Mr. Martinez-Fonts served as Special Assistant to the Secretary for the Private Sector at DHS. As Assistant Secretary, Mr. Martinez-Fonts is charged with providing America’s private sector with a direct line of communication to the Department. He and the Private Sector Office will work directly with individual business and through trade associations and other non-governmental organizations to foster dialogue between the private sector and the Department.

In April 2002, Mr. Martinez-Fonts retired as Chairman and Chief Executive Officer of JP Morgan Chase Bank in El Paso, Texas. Before moving to El Paso, he was President of the Bank in San Antonio. He began his 30-year career with Chemical Bank (a JP Morgan Chase predecessor organization) as a management trainee and worked his way through the organization as a lending officer in the Metropolitan Division and the International Division.

He has lived and traveled extensively overseas, including managing Chemical Bank’s offices in Manila, Philippines (1976-1979) and Mexico City, Mexico (1982-1988). He was Regional Manager based in New York of Chemical’s business in Argentina, Chile, Uruguay, Paraguay, and Bolivia (1980-1982).

Mr. Martinez-Fonts has served on many boards, including The Greater El Paso Chamber Foundation, Project ARRI-BA, ACCION International, and ACCION USA. He was a member of the Frito-Lay Hispanic/Latino Advisory Board, the United Way of El Paso Board, and the University of Texas at El Paso Development Board. In the past he also served on the Fannie Mae Advisory Board and the American Bankers Association Communications Council.

He served as 1993 Chairman of The Greater San Antonio Chamber of Commerce and 1988 President of The American Chamber of Commerce in Mexico City. He is the 1995 recipient of The National Conference of Christians and Jews Humanitarian Award.

Mr. Martinez-Fonts received his undergraduate degree in political science from Villanova University in 1971 and his MBA in finance from Long Island University in 1974.

Welcoming Remarks Dr. John B. Noftsinger, Jr., Vice Provost for Research and Public Service, James Madison University, and Executive Director, IIIA

Dr. Noftsinger serves as Vice Provost for Research and Public Service, Executive Director of the Institute for Infrastructure and Information Assurance, and Professor of Integrated Science and Technology and Education at James Madison University. He has primary responsibility for facilitating external grant and contract funding,

homeland security research programs, economic development, technology transfer, and academic public relations and service programs for JMU. He has led the development of an innovative bachelor’s program in Information Analysis at JMU and is actively engaged in developing economic acceleration policy and programs within the mid-Atlantic region through the Accelerating Innovation Foundation, Virginia Technology Alliance, and the Shenandoah Valley Technology Council, all of which he co-founded. He is a founding member of the Executive Committee of the Virginia Institute for

Defense and Homeland Security and Deputy Chairman of the University of Virginia’s Critical Incident Analysis Group (CIAG) Steering Committee. Dr. Noftsinger is also a member of the Critical Infrastructure Roundtable at the National Academy of Sciences. He serves as a Senior Fellow at the George Washington University Homeland Security Policy Institute (HSPI). In 2002, Dr. Noftsinger’s statewide leadership was recognized when he was appointed by Governor Mark R. Warner as co-chair of the Virginia Research and Technology Advisory Commission (VRTAC), which advises

the Governor and General Assembly of Virginia on appropriate research and technology strategies. He was also appointed by Governor L. Douglas Wilder as Deputy Secretary of Education for the Commonwealth for 1993-1994. He holds a bachelor of science in political science and public administration from James Madison University, a master of arts in higher education administration and student affairs from The Ohio State University, and a doctorate in higher education administration from the University of Virginia.

Dr. Linwood H. Rose, President, James Madison University

Dr. Linwood H. Rose, the fifth president in James Madison University's 96-year history, has led the University into a position of national prominence but has also represented JMU and Virginia in a variety of important roles on national, regional and state



commissions, committees and advisory boards.

President George W. Bush appointed Dr. Rose in the fall of 2002 to the National Infrastructure Advisory Committee. The committee makes recommendations regarding the security of the cyber and information systems of the United States. Governor Timothy Kaine appointed Dr. Rose to the Commonwealth of Virginia's Economic Development Strategic Planning Steering Committee, July of 2006.

Dr. Rose has served as chair of the Commission of Colleges and Schools

(SACS), the regional accrediting agency for eleven Southern states. He has also served as commissioner, Virginia state chairman, committee chair and executive council member for SACS. In addition, Dr. Rose served as a member of the Division I board of directors of the National Collegiate Athletic Association from 2000 until April of 2004.

He currently serves as the Virginia state representative to the American Association of State Colleges and Universities (AASCU).

He is a member and former president of the Council of Presidents, an organization of the presidents of Virginia's senior colleges and universities. He serves on boards of the American Shakespeare Center, the Shenandoah Valley Educational Television Corporation, The SunTrust Bank Western Division, the Harrisonburg Downtown

Renaissance Advisory Board, and the Virginia Institute of Government Advisory Committee.

Dr. Rose has also previously served as chairman of the

board of Rockingham Memorial Hospital; president and campaign chairman of the Harrisonburg-Rockingham County United Way; and as a member of the James Madison Commemorative Commission of the U.S. Congress.

Dr. Rose is an honorary member of Phi Kappa Phi Honor Society and a member of the Golden Key National Honor Society.

President Rose has been at James Madison University virtually his entire professional life. He began his professional career with JMU in 1975 and his assignments there

have included responsibilities in every division of the University. He took a leave from the University in the fall of 1985 to serve as Virginia's deputy secretary of education.

In 1994 he was promoted to the position of executive vice president. Dr. Rose served as acting president in the fall of 1997, and was chosen as JMU's chief executive in September 1998. He was formally inaugurated on September 17, 1999.

Born in Daytona Beach, Florida, Dr. Rose grew up in Staunton, Virginia. He earned his bachelor's degree in economics from Virginia Tech, his master's in educational administration and supervision from the University of Tennessee and his doctorate in higher education administration from the University of Virginia.

Panel One: Local Public-Private Partnerships

Moderator: Inspector Matthew J. Simeone, Jr., Moderator, former SPIN Administrator, Nassau County Police Department

Matthew J. Simeone, Jr. is an Inspector and twenty-three year veteran of the Nassau County Police Department (N.Y.) presently serving as the County's Task Force Against Gangs Coordinator, as well as Commanding Officer of Community Affairs.

In 2004, Inspector Simeone was instrumental in developing the Security/Police Information Network (SPIN), an all-crimes, all-threats, all hazards virtual public-private partnership which connects the Nassau County Police Department to more than 750 security directors and 125 community leaders. SPIN addresses homeland security, crime prevention, business continuity, and more, helping to make Nassau County the safest

Presenter Bios

community in the nation with a population of more than 500,000.

Before developing SPIN, Inspector Simeone spent several years as an assistant to the Commissioner of Police, five years as a community policing supervisor, and six years as a Police Academy trainer.

Inspector Simeone is a graduate of the 210th Session of the FBI National Academy and has a master's degree in Homeland Security from the Naval Postgraduate School's Center for Homeland Defense and Security. He is the author of "The Integration of Virtual Public-Private Partnerships Into Local Law Enforcement to Achieve Enhanced Intelligence-Led Policing" (Naval Postgraduate School Master's Thesis), as well as "The Power of Public-Private Partnerships: P3 Networks in Policing," which appeared in the May 2006 issue of *Police Chief Magazine*, as well as the April 2006 issue of the *FBI National Academy Associate Magazine*.

Ms. Oksana Farber, Vice President of Operations, Hiram Cohen & Son, Inc., and Vice Chair, Law Enforcement Liaison Council, ASIS International

Oksana Farber is Vice President of Operations, Hiram Cohen & Son, Inc., an insurance and risk management organization. She has over 25 years executive leadership experience and skills and is a profitability-oriented business strategist with expertise in Human Resources, Chief Security Officer responsibilities, and operations/facilities management. She is a published author in several security publications regarding building relationships post 9-11 to develop information-sharing programs and in HR publications about HR and Security Officers working together. Ms. Farber is an active member of ASIS International,

where she formerly served as New York City Chapter Secretary (2007) and currently (2008) serves as Vice Chair of the Law Enforcement Liaison Council.

Mr. Mario Doyle, CPP, Vice President, BuildingStar Security Corporation, Regional Vice President, ASIS International

Mario J. Doyle, CPP, serves as a Vice President with BuildingStar Security Corporation, one of the leading providers of security services in the New York and New Jersey metropolitan areas. Doyle has held several senior management positions with national and regional security firms and has developed a broad range of security management experience including corporate operations and compliance, personnel standards, quality assurance, training, problem solving and regional expansion. His areas of expertise also include developing security programs for colleges, airports, industrial, commercial, residential, healthcare facilities and government contracts.

In addition to being an established business executive, Doyle has been active in the law enforcement community for over a decade and has been a leader in promoting information sharing partnerships between the public and private sectors of law enforcement. He is a member of the Nassau County Police Department's Security Police Information Network and is a member of the Security Advisory Council, a coordinated crime prevention project that seeks to advance public safety and security through public/private partnership and cooperation. Doyle also serves as the Regional Vice President for ASIS International (ASIS), which is the largest organization for security professionals, with more than 34,000 members worldwide.

Doyle is a founding member of the Nassau County Law Enforcement Exploring Advisory Board, for which he also serves as co-chairman, and serves as a Director for the Nassau County Police Reserves, an organization with a mission to support the Nassau County Police Department. He is a licensed New York State private investigator and also serves as an officer on the board for the Associated Licensed Detectives of New York State (ALDONYS), a not for profit association comprised of New York State licensed private investigators and guard agency licensees. Doyle is also an active member of National Law Enforcement Associates, Inc., the Society for Human Resources Management (SHRM), the Association of Certified Fraud Examiners (ACFE) and the National Police Defense Foundation (NPDF).

Detective Sergeant William Leahy, SPIN Coordinator, Homeland Security and Counter Terrorism Bureau, Nassau County Police Department

Detective Sergeant William Leahy began his law enforcement career with the New York City Police Department in 1985. In October 1990 he joined the Nassau County Police Department, and upon graduation he was assigned to the Fifth Precinct as a patrol officer. After three years of patrol he was assigned to the newly formed Problem Oriented Policing Unit in the Fifth Precinct.

While in the P.O.P. Unit, Sergeant Leahy was the project leader for the "Illegal Massage Parlors / Houses of Prostitution" program. This innovative problem-solving project utilized local, state and federal laws in addition to civil penalties for property owners to rid the precinct and county of this blight. The program was recognized by the International Association of Chiefs

of Police and was a semi-finalist for the Webber Seavey Award for Quality in Law Enforcement. Additionally, Sergeant Leahy has been recognized by the National League of Cities and Police Executive Research Forum for excellence in Problem Oriented Policing.

Sergeant Leahy was promoted to the Detective Division and in 2004 he was promoted to the rank of Sergeant. A graduate of the FBI National Academy, Detective Sergeant Leahy is serving as the SPIN coordinator which is currently assigned to the Homeland Security Counter Terrorism Bureau.

Panel Two: All Hazards Consortium (Regional) Panel

Moderator: The Honorable Robert Crouch, Assistant to the Governor for Commonwealth Preparedness, Virginia

For the administration of Governor Timothy M. Kaine, Mr. Crouch coordinates the Commonwealth strategy and initiatives related to all-hazards preparedness. He is the Department of Homeland Security point of contact for the Commonwealth; Member, Senior Policy Group of the National Capital Region; Chair, Secure Commonwealth Panel; Vice-chair, Virginia Military Advisory Committee; Vice President, All Hazard Consortium Board; Member, Virginia Fusion Center Executive Board; Co-chair, Commonwealth Preparedness Working Group; Member, Virginia Citizen-Soldier Support Council; and Member, National Governor's Association Homeland Security Advisors' Council.

Prior to his appointment in the Kaine Administration, Mr. Crouch was Legal Counsel to Governor Mark R. Warner from May 2005 to January 2006. He served as Chief Deputy Secretary of Public

Safety, Warner Administration (January 2002-May 2005), during which time he served as Co-chair of the Commonwealth Preparedness Working Group; Co-chair, Critical Infrastructure Protection Working Group; Chair, Virginia Citizen-Soldier Support Council; and Chair, Interagency Anti-Gang Working Group. Mr. Crouch was a United States Attorney for the Western District of Virginia from 1993-2001. He was in private practice of law (1988-1993) in Charlottesville and Martinsville after receiving his J.D. from the University of Virginia. He received his B.A. in government from the University of Maryland and an M.P.A. from the University of North Carolina at Greensboro. Mr. Crouch served as Clerk of the Circuit Court, Henry County (resigned to attend law school), from 1976-1985.

Mr. Crouch is a former member of the George Mason University Board of Visitors, a former member and chairman of the Virginia State Community College Board and a former member of the Board of Directors of the Virginia Museum of Natural History.

Mr. David J. Lindstrom, M.A., CIPP/G, Chief Privacy Officer, Penn State; EMS Academic Programs Coordinator, Homeland Security Coordinating Council Member, Penn State; Secretary, All Hazards Consortium, Inc.

David is the Chief Privacy Office of Penn State University and academic coordinator for all Penn State EMS educational programs offered through the university. He is Secretary of the Board of Directors of the All Hazards Consortium, a corporation charged with enhancing all hazards programs and response for seven states and the District of Columbia.

In addition, David serves on the Advisory Board of the Medical Reserve Corps of Central Pennsylvania and is the Co-Chair of the Higher Education Knowledge Net of the International Association of Privacy Professionals.

David was Associate Director of Penn State's University Health Services and for 28 years responsible for all EMS activities at Penn State, academic and direct service delivery. In addition to daily EMS operations, David was in charge of EMS operations for all special events, including the 107,282 seat Penn State Beaver Stadium.

In the early 1970's, he was responsible for the development and implementation of EMT programs in 77 vocational technical schools and 16 Pennsylvania Community Colleges. In 1974, he served on the standard-setting committee of the National Academy of Science charged with defining the role of paramedics in pre-hospital care. In 1995, David co-authored the National Standard Curriculum for Paramedics and implemented paramedic this new curriculum throughout the United States.

David graduated from Indiana University of Pennsylvania with a B.S. in psychology in 1970 and a M.A. in counseling services in 1973. In 1970, David was commissioned as a U.S. Army Officer and served as a Combat Engineer until his honorable discharge in 1983.

Mr. John M. Contestabile Director of Engineering & Emergency Services at the Maryland Department of Transportation (MDOT)

John M. Contestabile has responsibility for the areas of Engineering Environmental Compliance, Rail Safety & Security and Emergency Response with the Maryland Department of Transportation. He has been with the Department for 29 years.

Presenter Bios

Mr. Contestabile has previously served on assignment with the Governor's Office as the Acting Deputy Director of the Office of Homeland Security, as well as in the capacity of Acting Assistant Secretary for Administration at the Department of Transportation. Mr. Contestabile serves on a number of National Committees, including Vice Chair of the American Association of State Highway and Transportation Officials Security Committee; the Transportation Research Board's Security Research Panel; the National Research Council's "Planning for Catastrophe" advisory panel; the National Academies study panel on the "Use of Transit during Evacuations;" and the Department of Homeland Security's "Safecom" Interoperable Communications Advisory Committee. He is a representative on the Board of the National Governor's Association for the Public Safety Spectrum Trust for the 700 MHz Broadband National License.

Mr. Contestabile received his bachelor of science degree in civil engineering from Worcester Polytechnic Institute in Massachusetts, and holds a master of business administration degree from the University of Baltimore. He and his wife and three children reside in Carroll County, Maryland.

Mr. Micheal Hughes, Northeast Program Development Manager, Northrop Grumman Corporation

Micheal Hughes is the Northrop Grumman Northeast Program Development. He is responsible for a full range of homeland security, public safety, transportation and health and human IT services. He works very closely with potential customers in the region to provide thought-leadership, best practices and lessons learned in IT services. He works with small business

partners for subcontracting opportunities. He has a bachelor degree from University of Maryland College Park and a masters degree from Johns Hopkins University.

Panel Three: National Security Telecommunications Advisory Committee Telecommunications/Electric Interdependency Panel

Moderator: Dr. John S. Edwards, Nortel's Designated Representative to the NSTAC's Industry Executive Subcommittee

Dr. Edwards' experience in the telecommunications field includes design, analysis, and business planning. He successfully created several design groups and founded four companies, one of which became a billion dollar subsidiary of a global corporation. He has held senior level management positions at small and large companies and has sound knowledge of telecommunications, computers and software.

Currently, Edwards is president of Digicom, Incorporated -- a position he has held since 1993. In this role, he also works as a consultant to Nortel Networks in the field of telecommunications security. Edwards has studied the security of the SS7 networks as they relate to the area of number portability and its relationship to the competition envisioned by the Telecommunications Modified Final Judgment act of 1984. The application of encryption and its export has been a topic of consideration as well. In addition to his Government advisory duties, Edwards has been a member of the board of directors of a small wireless communications corporation and assisted in the company's switching strategy. He designed the architecture and call processing plan for a wireless local loop system intended for the

export market, and he created a business plan and founded a telecommunications company to develop new wireless voice/data telecommunications equipment for sale to third world countries.

Edwards also advised various new telecommunications ventures on their architectures and design and was retained by a large telecommunications carrier in a telecommunication patent infringement case.

During his career, Edwards served as a Vice President for Technology Nortel Networks (1983-1993) where he was a senior technical leader in the U.S. Federal marketing sector. While there, Edwards secured over \$10 million in directed Government contracts. He represented Nortel Networks on key government/industry presidential committees, and chaired several committee task forces.

Other positions held by Edwards include Vice President for Engineering at TSS-Alcatel (1978-81), Co-founder and President of Digital Switch Corporation (DSC) (1976-78), Director of Advanced Design for DATRAN Corporation (1973-76), and other assignments with Bell Northern Research and Bell Telephone Laboratories. He served over two years as a Lieutenant in the U.S. Army Ordnance Corps where he designed the first combined voice/data communications system for the US Army, utilizing error detection/correction for the data communications element.

Edwards holds a bachelor of science degree in engineering physics and a masters of science degree in physics from the University of Illinois in Champaign. He completed further graduate studies in electrical engineering at New York University and earned his doctorate degree in electrical engineering at the University of Pennsylvania while under a Bell Laboratories support fellowship.

Mr. Daniel C. Hurley, Jr., Director, Critical Infrastructure Protection, U.S. Department of Commerce, National Telecommunications and Information Administration and Chair of the CDEP WG

Mr. Hurley serves as the Director, Critical Infrastructure Protection, in the U.S. Department of Commerce's National Telecommunications and Information Administration. A career member of the federal government's Senior Executive Service, he manages the Department's mission to ensure the Economic Security of Critical Infrastructure and leads the Department's participation in international initiatives to build cyber security capacity.

From 1993 to 2001 he served as Senior Advisor to the Under Secretary for Export Administration where he headed the Bureau of Export Administration's (BXA) nonproliferation and export control international cooperation initiative involving 25 countries in the New Independent States of the former Soviet Union and central European regions. As head of BXA's Foreign Industry Analysis Division from 1991 to 1993, he managed the preparation of foreign availability assessments as well as foreign industry analyses of militarily critical technologies. Between 1975 and 1991 Mr. Hurley was an attorney-advisor in the Department's Office of Chief Counsel for Export Administration.

Mr. Hurley holds B.S. and M.A. degrees in mathematics from St. Louis University. After serving as a Naval Officer in Southeast Asia, he earned his J.D. degree from Georgetown University. He also earned an M.B.A. in strategic management from George Mason University. Before retiring as a Captain in the U.S. Naval Reserve, Mr. Hurley completed senior courses at the Naval War College and the

National Security Agency and served as commanding officer of five naval reserve units.

Mr. Hurley and his wife Mary Ellen live in Fairfax County, Virginia, and have three grown children.

Mr. Lawrence C. Hale, Acting Director and Chief, Customer Service Division, National Communications System

Lawrence C. Hale became Acting Director of the National Communications System on January 4, 2008. Mr. Hale is responsible for planning and provision of national security and emergency preparedness communications for the federal government. In addition to his appointment as Acting Director, Mr. Hale continues his duties as the Chief of the NCS Customer Service Division, a position he has held since November, 2007. He joined the NCS having spent over two years as Chief Information Security Officer of Affiliated Computer Services, a Fortune 500 Information Technology company.

Previously, as Director of the Federal Computer Incident Response Center, he led the transition of that organization into DHS, and served as deputy director of the National Cyber Security Division's Computer Emergency Readiness Team (US-CERT).

In the U.S. Navy, he served as an information assurance action officer focusing on secure interoperability issues in the Joint Staff's Command, Control, Communications and Computer Systems Directorate (J-6). While at the Pentagon, he was a member of the Joint Staff Information Operations Response Cell during a number of cyber events and exercises which helped shape the U.S. government's computer security policy.

Hale was one of Federal Computer

Week's 2003 Federal 100 Award winners, recognized for his contribution as an information technology leader. In January 1999, he became the first military officer assigned to the National Infrastructure Protection Center (NIPC). While at the NIPC, he worked to improve the process of issuing warnings about cyber-related events and served on the Year 2000 (Y2K) task force in the Federal Bureau of Investigation.

Hale retired from the U.S. Navy as a Commander in May 2001. He has a master's degree in National Security and Strategic Studies from the Naval War College, and a master's in Aeronautical Science from Embry-Riddle Aeronautical University.

Symposium Recap

Dr. A. Jerry Benson, Vice Provost for Science, Technology, Engineering and Mathematics, James Madison University

Dr. A. Jerry Benson serves as Vice Provost for Science, Technology, Engineering, Mathematics, Health and Human Services, and Professor of Graduate Psychology. His primary responsibilities include oversight and coordination of the College of Integrated Science and Technology, the College of Science and Mathematics, the School of Engineering, and the Center for Science, Technology, Engineering and Mathematics Education Outreach. Dr. Benson has served the University in various administrative roles including Dean of the College of Education and Psychology and Dean of the College of Integrated Science and Technology prior to his present assignment. He holds a Bachelors of Arts in Psychology from Concord College, a Masters of Arts in Psychology (School) from George Peabody College for Teachers and a Ph.D. in Transactional Ecological

Presenter Bios

Psychology (APA approved combined-integrated clinical program) from George Peabody College for Teachers. Dr. Benson's principal areas of expertise and research include systems intervention, program evaluation and consultation.

Dr. Robert Reid, Dean, College of Business, James Madison University

Dr. Robert Reid is the Dean of the College of Business at James Madison University. The College of Business provides bachelors and masters degree programs for more than 3,500 students. As the leader of a team consisting of more than 150 faculty and staff, the College of Business provides exceptional educational opportunities for students. The College of Business faculty has been recognized for excellence in curriculum innovation, especially in the areas of curriculum integration and experiential learning.

Prior to becoming dean in 1996, he was the Department Head of Marketing and Hospitality Management. While in this role, he held the first J. Willard Marriott Professorship in Hospitality and Tourism Management. Before joining the faculty at James Madison University, he was an Associate Professor at Virginia Tech.

AACSB International accredits James Madison University's College of Business. This distinction places the JMU College of Business among the top 10 percent of business schools in the nation. The College of Business is a vibrant contributor to the success of the university, which in recent years has repeatedly been cited as one of America's finest predominately undergraduate universities by such publications as *USA Today* and *U.S. News and World Report*. In April 2006, *Business Week* ranked the College of Business 35th in the nation, from among 1,400 business schools.

Dr. Reid has conducted numerous

professional workshops and seminars for both public and private organizations. He has consulted with such organizations such as: The Colonial Williamsburg Foundation, ARAMARK, ITT-Sheraton, R.R. Donnelley, West Virginia University, Volvo-White, Celanese, and the National Restaurant Association.

He has authored or co-authored four editions of *Hospitality Marketing Management* and was a contributing author of two other books, *The Practice of Hospitality Management*, and *Introduction to Hotel and Restaurant Management*. Dr. Reid has written or co-authored over 40 journal and professional articles and was a recipient of an "Article of the Year" award presented by *The Cornell Hotel and Restaurant Administration Quarterly*.

He is actively involved in leadership positions with several professional and civic groups in which he has held various officer and board positions.

Poster Presentations in the Great Hall

The following research projects and highlighted partnerships are featured in the Poster Session in the Great Hall. Please visit with the researchers during session breaks and lunch.

EMERGENCY PREPAREDNESS AND RESPONSE: Disaster Identification Bracelet System (DIBS)



Depiction of the portable RFID scanning station.

A joint research effort between the Institute for Infrastructure and Information Assurance at James Madison University and RFID Informatics, Inc. has resulted in the development of a Radio Frequency Identification (RFID) system that tracks the current location of individuals evacuated to shelters in several different geographical locations during a natural disaster. This simple cost-effective

system will drastically reduce the agonizing time families spend searching for lost loved ones during an already difficult situation. It will also be used to facilitate effective distribution of food, medical supplies and other logistical needs in the eventuality of disaster.

Crisis Intervention Counseling Agent (CICA)

The Crisis Intervention Counseling Agent (CICA) is a knowledge-based, expert system (ES) agent whose function is to assist counseling personnel in providing timely, effective crisis intervention in field situations following a catastrophe. The CICA will be accessed by a web-based, hand-held, portable device that will also provide accurate and current information regarding hazards, site conditions, rumors and referral resources. As a result, outreach crisis workers will have immediate, consistent and essential information and expert advice for successful crisis intervention in the field setting.



Renewable Energy Demonstration Projects in the San Joaquin and Shenandoah Valleys

This research investigates the potential for the development of clean, renewable energy alternatives for Virginia that maximize the utilization of natural resources within the Commonwealth, while minimizing the overall environmental impact of Virginia's



energy and agricultural practices. Economic and environmental issues associated with the production, collection, and distribution of poultry litter are a major focus of this study, along an analysis of the potential to utilize the Harrisonburg Resource Recovery Facility to incinerate poultry litter and produce energy, and laboratory

investigations into the cultivation of freshwater and marine micro algae to reduce harmful emissions and generate high-value biomass for the production of biofuel.

Commission to Assess the Threat to the United States of Electromagnetic Pulse (EMP) Attack (the EMP Commission)

The electromagnetic pulse (EMP) generated by a high altitude nuclear

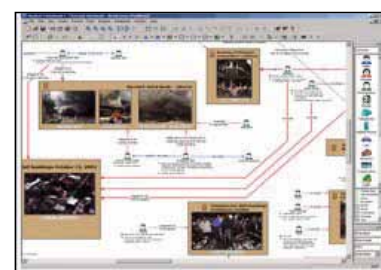


Starfish Prime was a high-altitude nuclear test conducted by the United States of America on July 9, 1962. The explosion took place 400 kilometers (250 miles) above Johnston Island in the Pacific Ocean. Unexpected effects were felt as far away as Hawaii 800 miles away.

explosion is one of a small number of threats that can hold our society at risk of catastrophic consequences. The increasingly pervasive use of electronics of all forms represents the greatest source of vulnerability to attack by EMP. Electronics are used to control, communicate, compute, store, manage, and implement nearly every aspect of United States (U.S.) civilian systems.

Problem Solving through Modeling

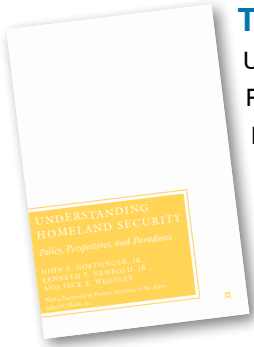
James Madison University's Institute for Infrastructure and Information Assurance has been helping communities and organizations solve problems through the use of modeling techniques. The focus is on problem solving – not on exercising a modeling philosophy. Therefore, the team combines different modeling methods depending on the problem to be addressed. Various tools (e.g. Stella, Vensim, Excel, i2's Analyst Notebook), and methodologies (system dynamics, mathematical modeling, agent-based modeling, fault tree



Poster Abstracts

analysis, social networks) are used to help find solutions. See the poster for three projects that illustrate three diverse problems and approaches: Intelligence Failure Analysis, Flu Pandemic Model, and Fault Tree Analysis Model.

New Understanding Homeland Security Textbook



Understanding Homeland Security: Policy, Perspectives, and Paradoxes by John Noftinger, Kenneth Newbold and Jack Wheeler of James Madison University is the first comprehensive academic text regarding homeland security. As a text for students of homeland security, public policy and terrorism studies, "Understanding

Homeland Security" explores the complex issues within the emerging domestic protection framework, providing current and future practitioners with a thorough view of the social, psychological, technological and political aspects that have shaped the growth of this movement. Understanding Homeland Security is published by Palgrave Macmillan.

Rapid Prototyping Product Realization Lab Capabilities



State-of-the-art manufacturing facility producing high quality rapid prototype models for start-up companies and established businesses. Provides solutions to meet specific

needs from design to production providing plastic (nylon) prototypes and limited-run plastic part manufacturing.

CyberCitz Project

This CyberCitz Project is organized around the ways middle schoolers are using the Internet. It integrates the ethical standards that can promote their use of the Web more wisely and responsibly. This project was produced in collaboration with the Virginia Department of Educational Technology and IIIA at JMU. This new project includes an Educators' Guide, a youth website, technology citizenship posters, and e-lessons on a K-12 learning management system. Learn more by visiting www.jmu.edu/iiia/cybercitz/.

Institute for National Security Analysis (INSA)

Our nation's greatest national security asset is also its most neglected: the reasoning methods of our analysts, strategists, and decision makers. The fundamental purpose of the INSTITUTE FOR NATIONAL SECURITY ANALYSIS (INSA) is to help transform that national reasoning so it can more adeptly engage unexplored, complex, and multidimensional challenges with innovative, rigorous, and transdisciplinary methods to produce proactive, reliable, and integrated solutions.

Also, look for presentations from these organizations:

The Infrastructure Security Partnership (TISP)
All Hazards Consortium (AHC)
National Defense Industrial Association
National Infrastructure Protection Plan (NIPP) Program Management Office
Mobile Satellite Ventures

Safety Security Ethics

CyberCITIZENSHIP

Enhance Your CyberCharacter

"The digital natives we teach need basic common sense about network safety and ethics. The JMU Cyber Citizenship Guide will be an excellent tool for teachers wishing to integrate basic net safety into their daily teaching."
— Joe Showker, ITRT Rockingham County Schools

WHAT? Your behavior—both online and offline—reflects your character. Choose to make good decisions regardless of your environment. Keep your reputation spotless.

HOW? Choose carefully what information you will share with the world. Keep personal stuff private.

WHY? Remember you only have one chance to make a good impression. When you put something on the Internet, digital footprints ensure nothing ever goes away.

Check out these things inside:
general Internet safety tips... social networking and communication technologies... surfing the web... gaming safely online.

Don't settle for just a virtual one. Get a real life!

This Guide was produced in collaboration with the Virginia Department of Educational Technology and the Institute for Infrastructure & Information Assurance at James Madison University.



Institute
for Infrastructure
and Information Assurance
at James Madison University

Current emergency evacuations are chaotic (2,600 children lost after Katrina evacuation, 330,000 families displaced.) About 1 million people were evacuated from their homes during recent California wildfires. Systems currently in place are insufficient.

EMERGENCY PREPAREDNESS AND RESPONSE: Disaster Identification Bracelet System (DIBS)

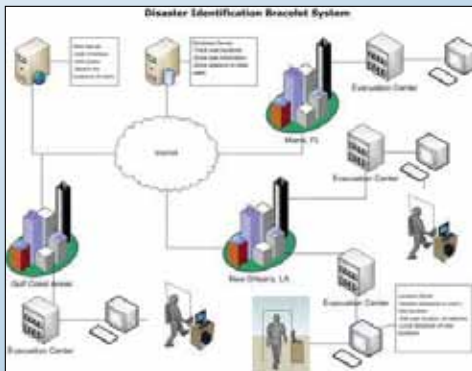
Patent Pending

summary... A joint research effort between the Institute for Infrastructure and Information Assurance at James Madison University and RFID Informatics, Inc. has resulted in the development of a Radio Frequency Identification (RFID) system that tracks the current location of individuals evacuated to shelters in several different geographical locations during a natural disaster. This simple cost-effective system will drastically reduce the agonizing time families spend searching for lost loved ones during an already difficult situation. It will also be used to facilitate effective distribution of food, medical supplies and other logistical needs in the eventuality of disaster.



Depiction of the portable RFID scanning station.

description... The system uses RFID-embedded bracelets that have been registered in a national secure database, and is driven by customized software. The great advantage of the system as a part of a pre-disaster planning initiative is its simplicity and effectiveness. Each individual wears a DIBS bracelet, which contains the uniquely encoded RFID tag. As the bracelet wearers pass by RFID reader stations, which are mobile and can be located at emergency shelter entrances, bus stations, airports, and other strategic locations, their bracelets will be automatically scanned, and the current date, time, and location will be logged in the database. This will enable related individuals to find one another by scanning their bracelets at DIBS kiosks at emergency shelters and immediately learn of each other's whereabouts. The system features automatic tracking and data logging, rapid information retrieval, a method for effective notification, and a centralized, secure data storage center housing the DIBS database that is accessible worldwide.



market significance... The system provides a simple and effective way for related individuals wearing the RFID bracelets to find one another during and immediately following a hurricane or other disaster emergency evacuation. The bracelets can also be used to retrieve family contact information if a young child is found separated from his/her parents, or to retrieve an unresponsive patient's medical information at a hospital. Additionally, the system will reduce the number of persons reported missing; reduce the time it takes to locate missing persons and reunite families; assist in the coordination of

emergency evacuations and aid distribution; help medical staff and first responders give proper aid; and better prepare whole communities to respond to emergency disaster evacuations.

stage... The system was developed in response to the disaster that accompanied Hurricane Katrina. It is easily scalable to serve communities with populations smaller than one thousand or larger than one million. The system can be readied for full scale deployment and implementation with several licensing modes available for interested communities.

keywords... disaster, hurricane, evacuation, emergency preparedness, emergency response, location system, notification system, track evacuees, national response plan

contact info... Dr. Anthony Teate, Professor, James Madison University, Dept. of Integrated Science and Technology, (540) 560-2712, teatea@jmu.edu



Photo credits
Photo 1: Ball State University:
<http://www.bsu.edu/up/article/0,1370,32363-2914-35954,00.html>
Photo 2: CommonCause.Org:
<http://www.commoncause.org/atl/cf/%7BF83C17E2-DD1-40F6-92BE-BD4425893665%7D.KATRINA%20RESCUE.JPG>

This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.





Institute
for Infrastructure
and Information Assurance
at James Madison University



Renewable Energy Demonstration Projects in the San Joaquin and Shenandoah Valleys

Public-Private Partnerships Pave the Way towards Energy Independence by achieving the goals of the 25 x '25 initiative 10 years ahead of schedule

The Problem: The United States consumes 25% of global oil production but contains less than 3% of the remaining global oil reserves within its boundaries.

OPEC controls 80% of all oil remaining on this planet. If the U.S. were to be cut-off from foreign oil imports, domestic oil reserves would be depleted within 2 years.

Globally, the demand for oil continues to grow while the remaining supply continues to shrink. Current projections that account for the rapid industrialization of both India and China forecast the depletion of global oil reserves within 25 years.

The problem lies in the fact that greater than 90% of the World's vehicles are powered by oil. This includes the tractors, trucks, trains, and boats used to produce the global food supply and delivery it to a growing global population. The oil-driven transportation sector is also responsible for the movement of all raw materials and all manufactured goods between factories and end-users around the world. The economic and social implications of the inevitable loss of oil are immense.

The Solution: The United States must act now.

The Department of Energy's roadmap calls for increasing the number of plug-in hybrid vehicles, but shifting transportation's energy load to the electric utility sector will require a massive increase in electrical generation capacity. Coal and nuclear will be part of the near-term solution, but because both of these resources are also limited in supply, they do not present a long term solution.

Long-term energy and environmental sustainability requires that the United States support the development and deployment of clean, renewable energy technologies. Wind, solar, hydrogeothermal, and biofuel options currently exist and are capable of addressing America's addiction to oil by displacing a significant portion of current consumption.

The 25 x '25 initiative calls for 25% of the United States' energy consumption to come from clean, renewable resources by the year 2025. To do this, but public must be educated about these forms of energy generation and shown that they can be deployed, successfully, on a large scale.



The 25x25 Vision: By 2025, 25% of America's energy consumption should come from clean, renewable resources. The San Joaquin Valley in California and the Shenandoah Valley in Virginia have been identified for their potential to serve as large-scale demonstration projects for the development and deployment of clean, renewable energy.

"If you can solve the education problem, you don't have to do anything else. If you don't solve it, nothing else is going to matter all that much!"
—Alan Greenstein, Outgoing Federal Reserve Board Chairman.

James Madison University : We don't just talk about it, we do it.

James Madison University President Linwood Rose (pictured right with Congressman Bob Goodlatte and Roy Blunt) has demonstrated a strong commitment to promoting America's energy independence. By mandating that clean, renewable energy be used in every single vehicle owned and operated by JMU, he has proven that we don't just talk about it, we do it.

By forming partnerships with the City of Harrisonburg and private industry, JMU and the surrounding area are able to run all of their vehicles on either biodiesel or ethanol blends. This includes ALL of the vehicles on campus and ALL of the City's public transportation (including school buses).





These partnerships have also resulted in the development of the Resource Recovery Facility, the only plant of its kind that converts the energy liberated from incinerating municipal solid waste into heat, air conditioning, and electricity. It also reduces the volume of trash that goes to the landfill by a factor of 3. In addition, JMU has established a 10 kW demonstration solar photovoltaic array and small-scale wind turbine that can supplement the University's electricity consumption demand.

The Center for Energy and Environmental Sustainability (CEES) within the College of Integrated Science and Technology promotes sustainable lifestyle, community, and business practices through research, education, and outreach. The Center conducts integrated studies of energy, natural resources, social needs, and economic development and is helping the Shenandoah Valley transform its future into one that is clean, renewable, and environmentally sustainable. More recently, CEES and the Presidential Commission on Sustainability has been tasked to evaluate all University practices in the context of reducing JMU's environmental impact and improving JMU's energy consumption habits. All of these items are then integrated into a comprehensive Science, Technology, Engineering, and Mathematics (STEM) educational curriculum that provides for a real-world, hands-on educational experience that promotes science literacy, prepares students for careers in an emerging alternative energy market, and helps them lead productive and meaningful lives.

Making the Shenandoah Valley Demonstration Project happen: Public-Private Partnerships are needed to unite this effort

President George W. Bush stated at the Washington International Renewable Energy Conference (WIREC) that America has got to change its energy consumption habits. At that same conference, Andy Karsner (Director of the Department of Energy's Renewable Energy and Energy Efficiency Program (REEEP)) stated that Federal funding to support alternative energy initiatives has arrived, totaling more than \$38 billion at his office alone. Lief Johansson, CEO of Volvo Truck followed Andy's statements by announcing that Volvo (the 2nd largest truck manufacturer in the world) has developed vehicles that will run on just about every type of alternative fuel currently in existence. The DOE wants to provide funding for demonstration projects so they can obtain real on-road data for their computer modeling. Volvo wants demonstration projects to prove their technology works. The American people need to see that these options are viable, economically and environmentally sound investments.

There are many reasons why the Shenandoah Valley is the perfect place for a large-scale renewable energy demonstration project. When combined with the efforts proceeded for the San Joaquin Valley in California, these two projects could serve as role models for the entire Nation. Below is a tabulated list of some of the reasons why the Shenandoah Valley is ideal for a demonstration of this magnitude:

- The Shenandoah Valley is in close proximity to Washington, D.C. - this area can easily be visited by State Legislators from all 50 states to show them, first hand, how to help America make the transition to renewable energy.
- The Shenandoah Valley is centrally located on the eastern seaboard - visitors from all over the East Coast would be able to see renewable energy in action.
- Bob Goodlatte, 11th District of Virginia (the Shenandoah Valley) has more Colleges and University than any other Congressional District in the United States and readily lends itself to wide-spread public education.
- The Shenandoah Valley is home to the Rt. 81 corridor, a major shipping route for the East Coast.
- Shenandoah National Park is the 3rd most polluted National Park - needs clean energy to change this.
- The Shenandoah Mountains are well-suited for Wind energy, Americans are currently looking at these options.
- It is home to Dominion's wood-fired powerplants that generates all of it's power from a clean, renewable resource.

It is now essential, for the large-scale implementation of renewable energy, to develop an educational program that promotes science literacy and facilitates the development of the next generation of scientists and engineers.












JAMES MADISON UNIVERSITY

College of Integrated Science and Technology

This research was supported [in part] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.



- The Shenandoah Valley hosts four of the top five agricultural counties in the state of Virginia and has tremendous biomass and landfill potential.
- Shenandoah Valley landfills are currently producing methane that can be used in a variety of renewable energy applications.
- SRI, the Stanford Research Institute is developing an Advanced Biofuel Research Center in the Shenandoah Valley.
- The largest Volvo Truck manufacturing facility is located in the Shenandoah Valley, the largest Volvo Truck Dealership is located here.
- Volvo has produce trucks, buses, and heavy-duty vehicles that can run on a wide variety of alternative fuels - they are looking for demonstration projects to see if proving grounds for their most innovative technologies.

- DOE press release



Crisis Intervention Counseling Agent (CICA)

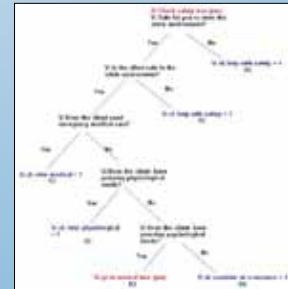
summary... The Crisis Intervention Counseling Agent (CICA) is a knowledge-based, expert system (ES) agent whose function is to assist counseling personnel in providing timely, effective crisis intervention in field situations following a catastrophe. The CICA will be accessed by a web-based, hand-held, portable device that will also provide accurate and current information regarding hazards, site conditions, rumors and referral resources. As a result, outreach crisis workers will have immediate, consistent and essential information and expert advice for successful crisis intervention in the field setting.



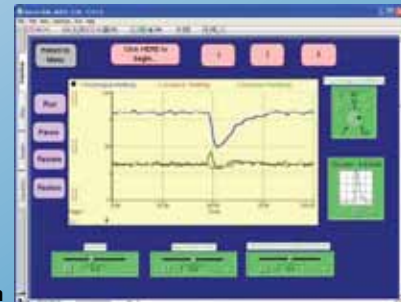
description... Whether highlighted by natural disasters like Katrina or human-made disasters like Darfu, there is a serious need to increase the crisis intervention counseling resources currently available to deal with the growing number of disasters confronting humanity. A promising resource is to use computer technologies, specifically intelligent systems and systems dynamics technologies, to provide real time assistance to human crisis intervention teams in disaster situations. Currently, on-the-scene assessment and intervention for victims of disaster events is provided by whatever counseling personnel and support infrastructure is available at the time in the event area. Success in responding to any given event is contingent on the practical experience, fact-based and theoretical knowledge, and assessment skills of the responding counseling personnel. At times, the discrepancies between needs and resources available present a seriously unsatisfactory situation that needs to be addressed. CICA will alleviate this situation by embedding the practical experience, fact-base and theoretical knowledge, and assessment skills of a crisis intervention expert. For example, an experienced, seasoned disaster intervener can walk into a crisis situation and immediately "see" what is wrong and in short-order respond with an "intuitively" appropriate intervention plan for the community in question. It is this kind of experience and expertise that will inform CICA and that, in turn, CICA will provide in crisis intervention situations.

CICA is being developed by a knowledge engineering team, working through the following objectives (sub-goals):

- develop, document and validate an expert system (ES) knowledge-base that will be the central repository of CICA's crisis intervention domain expertise;
- incorporate the ES knowledge-base into CICA, delivered as a web-based, hand-held device, with real-time access to current disaster event information;
- field test CICA and determine its utility when used by a variety of disaster relief teams and personnel;
- further develop and incorporate CICA into a tool to assist in training new crisis intervention professional.



market significance... Due to its geographic location, proximity to political power, and military installations, the Commonwealth of Virginia is at high risk for both natural disasters and acts of terrorism. Furthermore, the Shenandoah Valley will serve as an evacuation site for neighboring urban areas. Therefore, the Commonwealth and JMU have made a commitment to translate academic knowledge and technological expertise into practical emergency preparedness programs to protect our citizens. Deliverables from every stage of CICA's development can make contributions to disaster relief resources needed by the Commonwealth. CICA is a paradigm of translating academic knowledge and technological expertise into services for the Commonwealth; hence, a practical crisis intervention programs to protect our citizens.



stage... As described above, this project is still in the research and development stages. A working prototype for the first sub-goal has been completed, with significant progress made on the second sub-goal.

keywords... crisis intervention counseling, disaster relief counseling, artificial intelligence, intelligent agent, expert system, system dynamics thinking, complex dynamic systems

contact info... Joe Marchal, Director, Information Analysis Program, James Madison University, 540.568.2727 or marchajh@jmu.edu; Lennie Echterling, Graduate Psychology, James Madison University, 540.568.6522 or echterlg@jmu.edu



Institute
for Infrastructure
and Information Assurance
at James Madison University

Commission to Assess the Threat to the United States of Electromagnetic Pulse (EMP) Attack (the EMP Commission)

summary... The electromagnetic pulse (EMP) generated by a high altitude nuclear explosion is one of a small number of threats that can hold our society at risk of catastrophic consequences. The increasingly pervasive use of electronics of all forms represents the greatest source of vulnerability to attack by EMP. Electronics are used to control, communicate, compute, store, manage, and implement nearly every aspect of United States (U.S.) civilian systems.



Starfish Prime was a high-altitude nuclear test conducted by the United States of America on July 9, 1962. The explosion took place 400 kilometers (250 miles) above Johnston Island in the Pacific Ocean. Unexpected effects were felt as far away as Hawaii 800 miles away.

description...

Briefly, a single nuclear weapon exploded at high altitude above the United States will interact with the Earth's atmosphere, ionosphere, and magnetic field to produce an electromagnetic pulse (EMP) radiating down to the Earth and additionally create electrical currents in the Earth. EMP effects are both direct and indirect. The former are due to electromagnetic "shocking" of electronics and stressing of electrical systems, and the latter arise from the damage

that "shocked"—upset, damaged, and destroyed—electronics controls then inflict on the systems in which they are embedded. The indirect effects can be even more severe than the direct effects.

The EMP Commission under its original charter was charged with recommending steps that should be taken by the United States to better protect its military and civilian systems from EMP attack. Commissioners brought to this task a wide range of expertise, including service as an advisor to the President; senior management experience in both civilian and military agencies, national laboratories, and the corporate sector; and technical expertise in the design of nuclear weapons and in the hardening of systems against nuclear weapon effects.



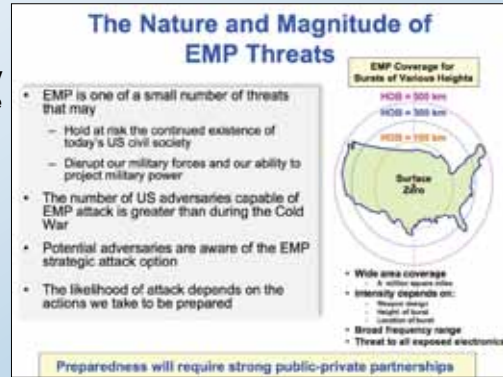
Long-term outage of electric power must be addressed.

The Commission worked with government and industry while also sponsoring workshops, equipment testing, analytical assessments to evaluate the threat on critical infrastructure elements such as equipment supporting the electric power distribution and management. A key concern from the analysis was on the potential long duration loss of electric power from an EMP attack over a wide geographic area. Electric power provides a base for operation of other infrastructures such as telecommunications and transportation. EMP could, compared to a nuclear attack on the city, kill many more Americans in the long run from indirect effects of collapsed infrastructures of power, communications, transportation, food, and water.

It is the view of the Commission that managing the adverse impacts of EMP is feasible in terms of time and resources. An EMP attack on the national civilian infrastructures would be a serious problem, but one that can be managed by coordinated and focused efforts between industry and government.

contact info... Dr. Michael J. Frankel, Executive Director-EMP Commission, 1710 SAIC Drive, Mclean, Va. 22102, michael.frankel@empcommission.org

Dr. George H. Baker, IIA Technical Director, 540-568-8767; bakergh@jmu.edu



Cellular network equipment testing



Automobile testing



Free-field illumination testing of digital equipment at Electromagnetic Simulator Facility





Institute
for Infrastructure
and Information Assurance
at James Madison University

Problem Solving through Modeling

James Madison University's Institute for Infrastructure and Information Assurance has been helping communities and organizations solve problems through the use of modeling techniques. The focus is on problem solving – not on exercising a modeling philosophy. Therefore, the team combines different modeling methods depending on the problem to be addressed. Various tools (e.g. Stella, Vensim, Excel, i2's Analyst Notebook), and methodologies (system dynamics, mathematical modeling, agent-based modeling, fault tree analysis, social networks) are used to help find solutions. The following three projects illustrate three diverse problems and approaches.

Intelligence Failure Analysis

In Summer 2008, five students and two staff members will utilize i2's Analyst Notebook and System Dynamics Modeling to explore failures in intelligence analysis. Ten to twelve failures will be modeling in Analyst Notebook. These models will show both a time line of activities (when did we know what?) and any social network of people involved - enemies, analysts, and policy makers. The intent is to understand how the failure manifested and why. Was it simple ignorance of key information? Did we underestimate the enemy? Did we not recognize the extent of the enemies intent?

After the initial examination of a dozen failures, analysis of commonalities within these failures will be explored. If it is determined that patterns are starting emerge in the analyst behaviors, additional failures will be explore. Ultimately, with a large enough pool, the true behavior of intelligence analysis can be explored and improved.

stage... Initial

market significance... This project is specifically for a client interested in improving their intelligence analysis methodology.



Flu Pandemic Model

In the Winter and Summer of 2007, four students and several staff member engaged with a local hospital to understand how a flu pandemic would impact hospital work. After many discussions it was evident that the hospital's focus was on determining when staffing levels are too low to provide adequate care to the patients. Each hospital may define that line in different places. The model developed allows changes to the various parameters that describe the hospital staffing and patient flow. Output from the model allows the hospital to identify when they are 'in trouble' as defined by their standards. In the Spring of 2008, this tool was used to facilitate a Catastrophic Event Planning Workshop for the Shenandoah Valley in conjunction with the Virginia Department of Health.

stage... Software available

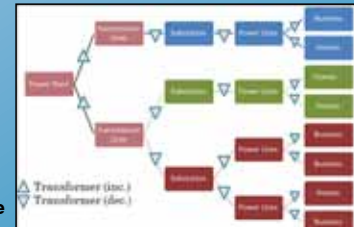
market significance... Health Care. This project was developed for a specific client. The software design and code can be modified to add functionality.

Fault Tree Analysis Model

This model is underway (Summer 2008). This software will enable the user to create simple to complex fault tree diagrams, including time to repair elements in the tree. When a fault occurs, the system will identify the time it takes to 'recover' the system. Multiple faults may be instigated to identify the overall time to achieve full recovery. This model will incorporate probabilistic risk analysis related to overall time to recovery. Future plans include using this software to instigate discussion and more complex modeling around scarce resource allocation. Time is a critical component but if there is a limited resource, how does one allocate the material? This model is the first step in examining the possibility of modeling the human component of scarce resource issues (i.e. who gets the scarce resource? Those with the most power? The government? Those who have the greatest need? How would we define 'need'? etc.) A secondary research component of this project is research into virtual reality (Second Life, etc.) where players can react to a scarce resource issues. For example, if a major power failure occurs through an EMP strike where multiple transformers are damaged, how will players negotiate the allocation of electrical transformer parts (limited resource)?

stage... Initial (Fault Tree Analysis Software should be complete by end of August. Further modeling in Second Life is TBD.)

market significance... Disaster Recovery Planning



contact info... Patricia Higgins, Associate Director, Information Analysis and Modeling, Institute for Infrastructure and Information Assurance, James Madison University, 540-568-1727 or higginpe@cisat.jmu.edu

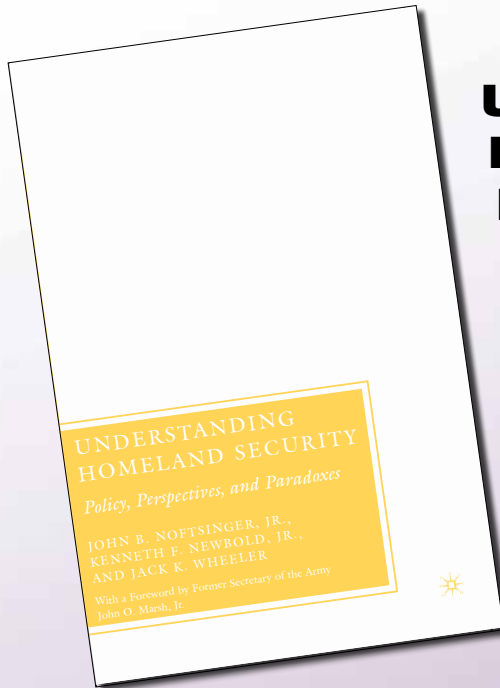
This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.





Institute
for Infrastructure
and Information Assurance
at James Madison University

***New Book to be
Released May 2007***



Understanding Homeland Security: Policies, Perspectives, and Paradoxes

JOHN B. NOFTSINGER, JR.,
KENNETH F. NEWBOLD, JR.,
AND JACK K. WHEELER

With a Foreword by Former
Secretary of the Army
John O. Marsh, Jr.

With the mounting threat of terrorist attacks, natural disasters, and cascading technological failures, the United States has been forced to address vulnerabilities and bolster homeland security efforts. *Understanding Homeland Security: Policy, Perspectives, and Paradoxes* provides the first truly comprehensive analysis of the historical, social, psychological, technological, and political aspects that form the broad arena of homeland defense and security. Utilizing an interdisciplinary approach, the text provides a view of past events and how they formed the terrain for current events, giving the reader a detailed knowledge of government response and policy implications. With both the public and private sectors investing heavily in protection efforts, this text offers the essential starting point for the dynamic and emerging homeland defense and security arena.

"To illuminate Homeland Security is an ambitious undertaking in a world where the topic often generates more heat than light. Through integration of governmental, business, and academic perspectives, the authors succeed in providing the reader with a vital framework for understanding. I know of no other single source that provides students and policy makers with such a thorough, yet eminently readable volume."

—GREGORY SAATHOFF, M.D., Executive Director, Critical Incident Analysis Group (CIAG),
University of Virginia School of Medicine

"Finally, a comprehensive and coherent textbook for the homeland security arena. The authors have undertaken a complex subject matter and distilled it into a presentable format that will have great utility from the classroom to the boardroom. The balancing and integration of subjects that impact public and private sector organizations as well as academia provide the instructor and student with a unique text that will also serve as a ready reference long after the class has concluded."

—PAUL M. MANISCALCO, MPA, Gilmore National Terrorism Commission, Chairman,
Threat Reassessment Panel and State and Local Response Panel

This research was supported (in parts) by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.





Institute
for Infrastructure
and Information Assurance
at James Madison University

Rapid Prototyping Product Realization Lab Capabilities

summary... State-of-the-art manufacturing facility producing high quality rapid prototype models for start-up companies and established businesses. Provide solutions to meet specific needs from design to production providing plastic (nylon) prototypes and limited-run plastic part manufacturing.



description... This state-of-the-art manufacturing lab produces high quality rapid prototype models for business, education and industry. This lab provides solutions to meet specific needs from design to production providing plastic (nylon) prototypes and limited-run plastic-part manufacturing. From a hand-drawn sketch, a picture image, or a computer drafted design, this lab can create a 3D solid that can evolve into a prototype. Models are drafted from scratch using AutoCAD, Inventor, SolidEdge, Magics, and Cobalt. Additionally, we can easily convert files generated in many other CAD software.



market significance... To stay competitive in the global marketplace, businesses recognize the benefits of rapid tooling technologies. This lab can produce a single prototype for further design and testing, or small batch quantities of functional plastic parts. This process offers significant reduction in time from idea to part, allowing the company to stay a step ahead of the competition. This is a great place for entrepreneurs to create their invention as a prototype and test the marketplace with a limited run of product.

stage... We offer product design assistance, computer aided design, rapid prototyping, injection molding, and machining capabilities. Industries served include: appliance, electrical, medical devices, education, entertainment, marine, tool, and water purification.

keywords... rapid prototyping, 3D solid prototypes, AutoCAD, manufacturing, injection molding

FOR MORE INFORMATION, CONTACT:

Dwight Dart

Center for Performance Manufacturing Product Realization Lab

701 Carrier Drive | Harrisonburg, VA 22807

www.chpm.jmu.edu | 540.568.2545 | dartdr@jmu.edu

© 2007 James Madison University ALL RIGHTS RESERVED

This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.



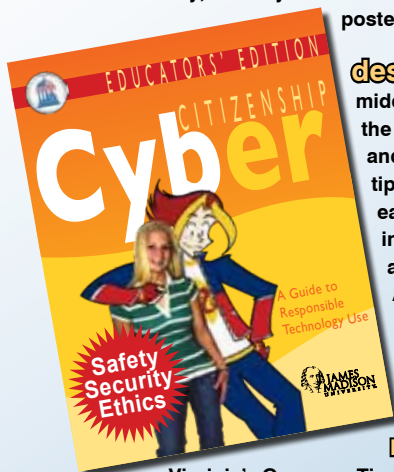


Institute
for Infrastructure
and Information Assurance
at James Madison University



CyberCitizenship Project

summary... Organized around the way middle schoolers use the Internet, the CyberCitz Project provides teaching materials on Internet safety, security and ethics. This new project includes an Educators' Guide, a youth website, technology citizenship posters, and e-lessons on a K-12 learning management system.



description... This project is organized in a way that addresses the ways middle schoolers are using the Internet. The Educators' Guide integrates the ethical standards that can promote their use of the Web more wisely and responsibly. It includes information everywhere from general safety tips to social networking and gaming. The youth edition of the guide will be easily available to students through an interactive website, targeting the information presented in the educator's version. Customizable e-lessons are currently being developed for a K-12 learning management system. A series of technology citizenship posters are also available.

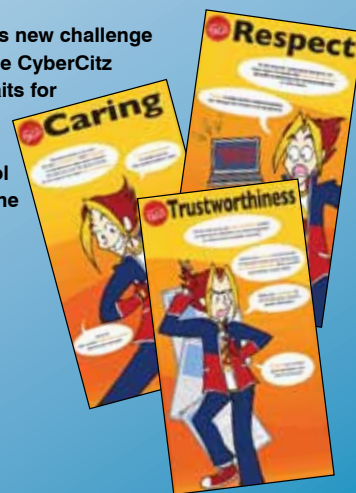
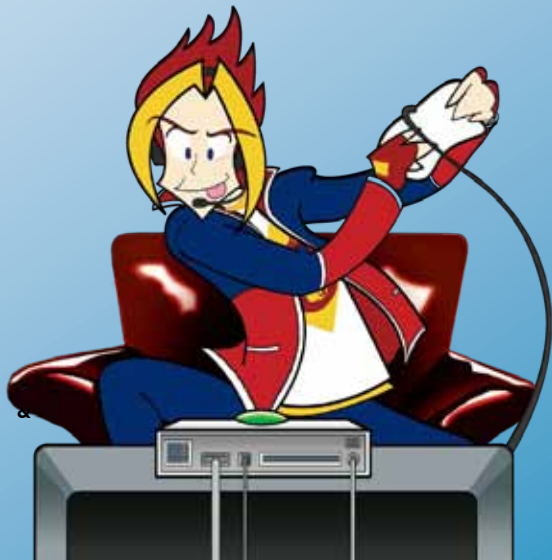
This project was produced in collaboration with the Virginia Department of Educational Technology and IIIA at JMU. Learn more by visiting www.jmu.edu/iiia/cybercitz/.

market significance... Legislation passed in 2006 and signed by Virginia's Governor Timothy Kaine added a new component to K-12 education curriculum to implement instruction on Internet safety for all students. The Legislation also required the Superintendent of Public Instruction to issue guidelines to school divisions in regards to instructional programs related to Internet safety. The Virginia Department of Educational Technology released "GUIDELINES AND RESOURCES FOR INTERNET SAFETY IN SCHOOLS" (<http://www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines.shtml>) to guide educators as they created programs to meet this new challenge.

To further assist in effectively implementing the new law into the classroom, IIIA took this new challenge further than VDOE could by creating hands-on materials designed for middle school. The CyberCitz project adds ethics to the mix by developing a series of posters on positive character traits for technology use.

stage... The Educators' Guide is being distributed to all middle schools and each school district in Virginia. The youth version (website) is currently under development, as are the e-lessons for the learning management system.

keywords... Internet Safety; safety, security and ethics; K-12 education



The CyberTag Posters were produced to augment the Internet Safety Guidelines from the Virginia Department of Educational Technology. CyberCitz Tags were developed by Joe Showker, Rockingham County Public Schools. Used by Permission. © 2007 Institute for Infrastructure & Information Assurance at James Madison University. ALL RIGHTS RESERVED

contact info... Cheryl J. Elliott, Assistant Director for Marketing External Relations, IIIA, 540-568-4442, elliottcj@jmu.edu

This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.





INSTITUTE FOR NATIONAL SECURITY ANALYSIS *at James Madison University* STRATEGIC VISION

OVERVIEW OF INSA:

Our nation's greatest national security asset is also its most neglected: *the reasoning methods of our analysts, strategists, and decision makers*. The fundamental purpose of the **INSTITUTE FOR NATIONAL SECURITY ANALYSIS (INSA)** is to help transform that national reasoning so it can more adeptly engage unexplored, complex, and multidimensional challenges with innovative, rigorous, and transdisciplinary methods to produce proactive, reliable, and integrated solutions.

External support for the Defense and Intelligence Communities (from academia or business) often offers one of three types of assistance: a) new technologies to improve the collection and/or exploitation of data, b) policy-making support through high-level strategic proposals, or c) complete analysis in the form of outsourced analysis on specialized topics. By contrast, INSA offers support for the most central (and neglected) element of Defense and Intelligence analysis: *the cognitive process by which analysts reason to well-justified conclusions for their decision makers*. The majority of intelligence failures evolve from errors in the reasoning process of analysts. Yet, that reasoning process is typically taken for granted in favor of technology, policy, or specialized subject matter expertise. Hence, **instead of trying to support the Defense and Intelligence Communities by telling analysts WHAT TO THINK**, INSA seeks to support them by educating analysts **HOW TO THINK**.

OBJECTIVES OF INSA:

The strategy of **INSA** is to *discover*, *develop*, and *deliver* new methods of critical thinking and reasoning to our national security community:

1. *Discover* the most fundamental structural challenges to effective reasoning in national security along with rigorous and relevant methods to address them.
2. *Develop* an innovative new model of advanced critical thinking and reasoning specifically designed to address the fundamental reasoning challenges in national security.
3. *Deliver* completed reasoning methods *directly to national security community* (via select national security partners) by means of a) resources for analysts, strategists, and decision makers such as “analyst guides” and professional-improvement publications, b) resources for national security training/education departments such as “curriculum guides” and educator-improvement publications, and c) support for education and training programs across the Defense and Intelligence Communities (where appropriate) through related internal training and educational bodies.



Dr. Noel Hendrickson
Director
hendrinx@jmu.edu

Amy M. Ballard
Operations Coordinator
ballaram@jmu.edu



HOST Contact Information:

Federal Facilities Council

Lynda Stanley
Director, Board on Infrastructure and the Constructed Environment
National Research Council
500 Fifth Street, NW, Room 943
Washington DC 20001
Phone: 202-334-3374; Fax: 202-334-3370; lstanley@nas.edu
www.nationalacademies.org/bice

IIIA Advisory Board

The mission of the Institute is to facilitate development, coordination, integration, and funding of activities and capabilities of the James Madison University academic community to enhance information and critical infrastructure assurance at the federal, state, and local levels. The Institute is guided by an advisory board that includes a distinct group of individuals representing business, industry and government.

Mike Becraft, SI International, Inc.
Daniel Caprio, D.C. Strategies, LLC
Robert Cofod, BankDetect
Grant Cooley, Tele-Consultants, Inc.
Raghu Dev, Oracle Corporation
Kevin Esser, Predicate Logic
Chaz Evans-Haywood, Clerk of the Circuit Court,
Harrisonburg and Rockingham County
Gene Garlick, Northrop Grumman Information Technology
Mike Hutton, National Counterterrorism Center
Matthew Keller, Corsec Security, Inc.
Michael King, Northrop Grumman Information Technology
Ken Knight, Office of the Director for National Intelligence
Jacqueline Gamblin, Ingenium Corporation
Richard G. Little, Keston Institute for Infrastructure & Policy,
University of Southern California,
Sadaat Malik, Cisco Systems, Inc.
Louis McDonald, Virginia's Center for Innovative Technology
Bill McGilvery, i2, Inc.
Jeffrey Payne, Cigital, Inc.
Brendan Peter, LexisNexis Special Services, Inc.
Ben Plowman, Luna Innovations
John Rice, United States Navy, COMOPTEVFOR
Kyndra Rotunda
Fenton "Dutch" Thomas
Jay Willer, Blue Ridge Home Builders Association

James Madison University

Dr. John B. Noftsinger, Jr.
Vice Provost for Research and Public Service; Executive Director, IIIA
MSC 4107, Harrisonburg, VA 22807
Phone: 540-568-2700; noftsijb@jmu.edu
www.jmu.edu/research

Dr. George H. Baker
Technical Director, IIIA
MSC 4102, Harrisonburg, VA 22807
Phone: 540-568-8767; bakergh@jmu.edu

Ms. Amy Ballard
Administrative Assistant
MSC 4111, Harrisonburg, VA 22807
Phone: 540-568-3640; ballaram@jmu.edu

Mr. Benjamin T. Delp
Assistant Director for Administration and Public Policy, IIIA
MSC 4111, Harrisonburg, VA 22807
Phone: 540-568-1661; delpbt@jmu.edu

Ms. Cheryl J. Elliott
Assistant Director for Marketing and External Relations, IIIA
MSC 3804, Harrisonburg, VA 22807
Phone: 540-568-4442; elliotcj@jmu.edu

Dr. M. Hossain Heydari
Associate Director for Information Assurance, IIIA
MSC 4103, Harrisonburg, VA 22807
Phone: 540-568-8745; heydarmh@jmu.edu

Ms. Patricia Higgins
Associate Director for Information Analysis and Modeling, IIIA
MSC 3804, Harrisonburg, VA 22807
Phone: 540-568-1727; higginspe@jmu.edu

Mr. Steve Knickrehm
Associate Director for Policy, IIIA
Assistant Professor of Health Sciences
MSC 4301, Harrisonburg, VA 22807
Phone: 540-568-3497; knickrsc@jmu.edu

Mr. Kenneth F. Newbold, Jr.
Director of Research Development
MSC 4111, Harrisonburg, VA 22807
Phone: 540-568-1739; newbolkf@jmu.edu

Mrs. Rebecca L. Rohlf
Fiscal Technician
MSC 4111, Harrisonburg, VA 22807
Phone: 540-568-3640; rohlfrl@jmu.edu

IIIA Graduate Fellows:
Ryan Cornett (cornetrp@jmu.edu)
Avery Daugherty (daugheac@jmu.edu)

About Your Hosts...

The **Federal Facilities Council**

www.nationalacademies.org/ffc/

The Federal Facilities Council (FFC) was established in 1953 as the Federal Construction Council. It operates under the auspices of the Board on Infrastructure and the Constructed Environment (BICE) of the National Research Council, the principal operating agency of the National Academies and the National Academy of Engineering.

The FFC's mission is to identify and advance technologies, processes, and management practices that improve the performance of federal facilities over their entire life-cycle, from planning to disposal.

- develops and disseminates facilities-related information through Networking, conferences, workshops, and studies;
- provides a forum to identify government-wide issues regarding facility planning, design, construction, operation, maintenance, and management;
- convenes standing committee meetings to promote networking and information sharing among sponsor agencies;
- deploys its findings through its reports published by the National Academy Press.



The **Institute for Infrastructure and Information Assurance**

www.jmu.edu/iiia/



Institute
for Infrastructure
and Information Assurance
at James Madison University

The Institute for Infrastructure and Information Assurance (IIIA) facilitates development, coordination, integration and funding of activities and capabilities of the James Madison University academic community to enhance information and critical infrastructure assurance at the federal, state and local levels. IIIA emphasizes collaborative interdisciplinary research that focuses on developing technologies with student participation and that have potential for public benefit and possible commercialization. Further, the Institute focuses on the integrative, interdisciplinary nature of real-world problems and strives to bridge traditional academic departments to develop solutions to the critical security problems facing our nation. IIIA partners with George Mason University on the Critical Infrastructure Protection Program (CIPP). IIIA Vision is a society strengthened and enriched by increasingly dependable infrastructure fostered by a strong university role in leadership, interdisciplinary education, research and problem-solving.



James Madison University is a comprehensive co-educational institution of higher learning in the Shenandoah Valley of Virginia. The University comprises the Colleges of Arts and Letters, Business, Education, Integrated Science and Technology, Science and Mathematics, and Graduate and Professional Programs. JMU offers 66 undergraduate degree programs, as well as 29 master's, two educational specialist, and four doctoral majors. JMU is dedicated to the belief that an enduring and meaningful educational experience must be future-oriented, grounded in knowledge of one's cultural heritage learned from study in the liberal arts and sciences.