May, 2006

Homeland Security: Engaging the Frontlines - Symposium Proceedings

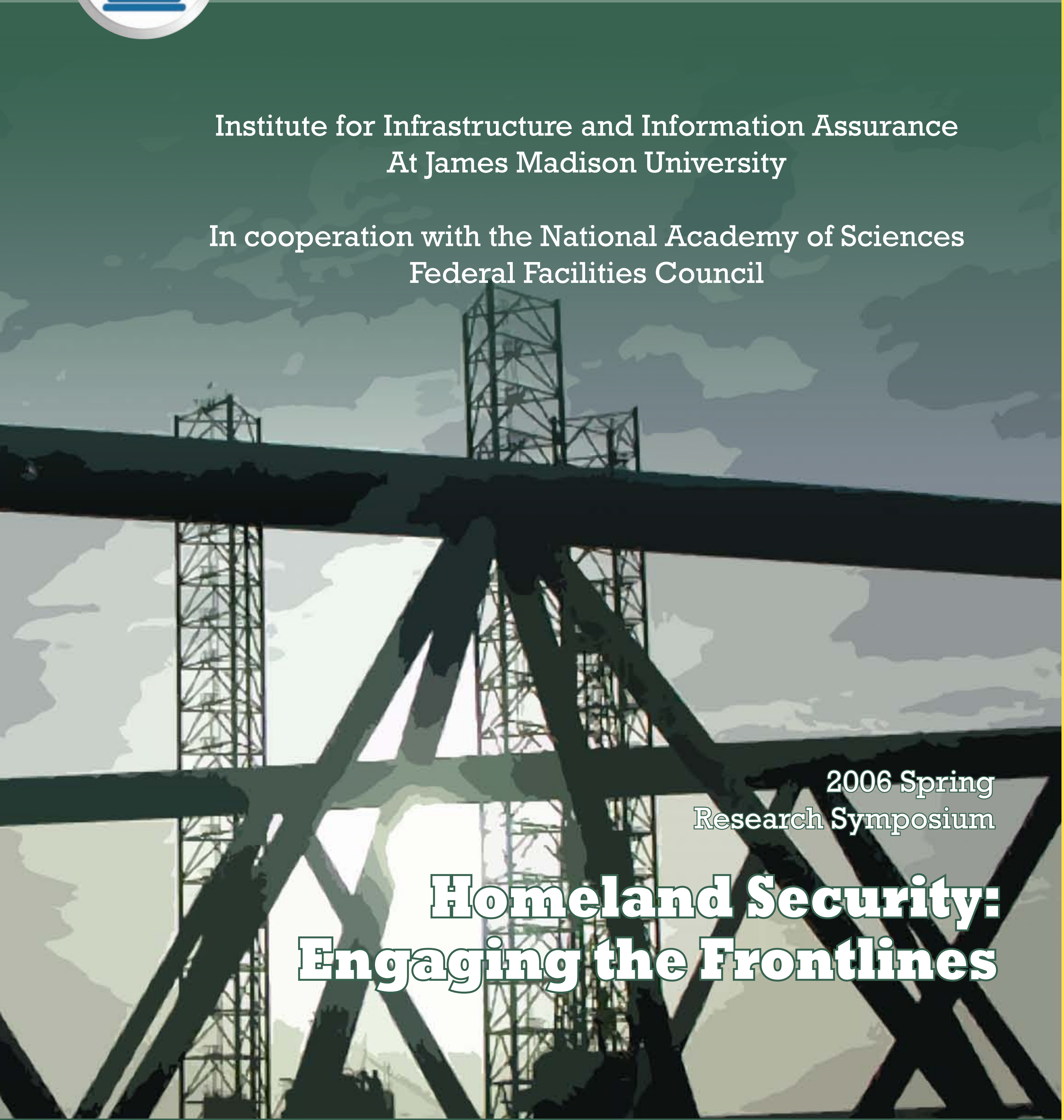
George H Baker, *James Madison University*
Cheryl J Elliott, *James Madison University*

Homeland Security Symposium

PROCEEDINGS

Institute for Infrastructure and Information Assurance
At James Madison University

In cooperation with the National Academy of Sciences
Federal Facilities Council



2006 Spring
Research Symposium

Homeland Security: Engaging the Frontlines

JAMES MADISON UNIVERSITY

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

2006 Spring Research Symposium
Homeland Security: Engaging the Frontlines

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

May 12, 2006

George H. Baker
Cheryl J. Elliott
Editors

Institute for Infrastructure & Information Assurance
James Madison University
Harrisonburg, Virginia

IIIA Publication 07-02

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 Analysis

www.jmu.edu/iiia/

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 closely 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.

Edited by George Baker and Cheryl J. Elliott
Graphic Design by Cheryl J. Elliott, Danny Cohen
Additional Transcription by Cameron Clark

Printed in the U.S.A.

IIIA Publication 07-02

Contents

Introduction

The rise of the American homeland security endeavor under the leadership of the new Department of Homeland Security has been heralded by several major national strategy documents. These documents have served to organized efforts at top levels within the government and industry. However, the national strategy guidance is not getting to many organizations and people at the grass-roots level who can make the most difference in preventing attacks, protecting systems, and recovering from catastrophic events, viz. the general citizenry, private infrastructure owners, and local governments.

To better understand grass-roots issues and solutions, James Madison University, in cooperation with the Federal Facilities Council, organized this symposium, bringing together a cross-section of federal, state, and local officials as well as industry, academia, and citizenry. Specific symposium objectives included:

- Illumination of current strategies and efforts and their strengths and shortfalls
- Exposition and discussion of new strategies to engage and incentivize organizations and individuals on the frontlines including threat awareness, prevention, protection, and response.

Emergent Themes

From the "Engaging The Frontlines" Proceedings

The Homeland Security endeavor necessitates a strong role for collaboration among government, academe, the private sector, and nonprofit organizations. The symposium, by design, brought together diverse communities including government, academia and industry. It served as a forum for sharing information on topics of research related to homeland security including protection, prevention, and response particularly as related to people on the "front lines" of homeland security. Despite the varied backgrounds of panelists and keynote speakers, we are excited about the important common themes from the proceedings that were reinforced by several presentations representing multi-discipline perspectives. These themes relate to clarification of who are the frontlines, improving the coordination chain from local to state to federal authorities, balanced preparedness for normal/natural disasters vs. malicious incidents, disaster planning guidance, the importance of attention to human psychology in planning and response, and the importance of coordinated assessments. Of course, the most important part of the proceedings are many ideas concerning future directions - what we can do better in our quest for a more unified, seamless national-to-local homeland security fabric. We have distilled common ideas from presentations below.

1 A better-prescribed balance of responsibilities is needed among Federal, State, and local governments/businesses.

We need to shift focus away from dependence on the federal government during disaster situations. The federal government is not set up to do it all. It should serve in a top-level leadership and coordination role. At the top level, we need identifiable people within the Homeland Security Council and DHS with authority to address regional-scale threat issues. But it is more important to energize local governments, business leaders and private citizens to invest in preparedness including the protection of critical infrastructure. And individual citizens must take personal responsibility for family preparedness.

The National Infrastructure Protection Plan outlines a top-down strategy. The plan is not prescriptive enough on the chain of responsibility reaching forward to the front lines - the local "grass-roots" level. A prescribed thread of continuity is needed concerning the division of responsibilities among state/local government and private infrastructure service providers. The national plan will succeed only to the extent that the local level infrastructure owners and operators are motivated to become part of the process and understand their roles in the grand scheme. It is important to push the planning down to the lowest level. Every emergency is a local emergency and local protection and preparedness planning are keys to successful recovery. The grass-roots level understands the critical systems and their vulnerabilities best and will be the earliest responders.

Community level planning should involve local leadership in government, business, the medical community, the legal community, civic organizations, and faith-based groups. Planning for a faster, more effective response should also involve the general public. We need a "community-based-national" preparedness. In any high consequence event, the first line of defense is us. Us, as an alert cadre of private citizens and local businessmen. The Homeland will be secure when our hometowns are secure. This is somewhat the antithesis of the Homeland Security Act.

2 Better communication is needed among all levels, but particularly to and within the grass-roots level.

The public is not well-informed concerning how they fit into the national homeland security strategy. At the national and state levels we tend to view physical, chemical, biological, and cyber issues of homeland security from a perspective at 10,000 feet. Our national strategy documents have tended to focus on a top-down approach to homeland security. There needs to be a commensurate bottom-up approach that meshes with the national strategy.

Public communication requirements span all high consequence event timeframes including pre-event preparedness, trans-event response and coordination, and post-event recovery. The public is not aware of national strategy and is not getting all the information needed to prepare and respond.

Relative to trans-event contingencies, there has been an enormous amount of work done in risk communication, particularly risk communication related to natural hazards. However there is more involved than getting the message out to people concerning what bad things could happen. We must cultivate an organizational culture that is receptive to the message. We can have the best analysts in the world but if they're operating in a culture that is not receptive to things that run counter to what authorities want to hear, we won't get good results. The Challenger and the Columbia space shuttle disasters, the Northeast Power blackout, catastrophic bridge failures, and Katrina are all examples of this phenomenon. In these cases, there was known predictive information, there were reactions based on rules of order and people failed to act because of organizational-cultural issues.

It is also important to reduce action lag time. People are skeptical of public pronouncements. The issue is "who do they trust and who do they believe?" No system will be perfect, but we can certainly do better. This is an area that doesn't need better research – it needs better implementation.

While we need better communication to first responders, we also need to avoid information overload. Too much detail can actually be counterproductive, leading to paralysis. We provide front line people with a lot of planning information but we haven't done a good job of helping them sustain a minimum set of essential skills. A surplus of information, much of it wrong, results in paralysis.

Equipment interoperability is important to communications. Field experience shows that interoperability is not about buying a lot of technology. It's really about relationships. We must build our technology around the relationships we form.

Education and training are an important element of better communication. A quote from Thomas Jefferson is profound in this regard: "I know of no safe depository of the ultimate powers of the society but the people themselves; and if we think them not enlightened enough to exercise their control with a wholesome discretion, the remedy is not to take it from them but to inform their discretion."

We need to educate the local level, going beyond green/amber/red alerts. Because Americans have short memories, it is important to keep the threats and consequences in front of the public. The public must be informed of simple, procedural measures to prepare for and respond to disasters. Universities need to do a better job of packaging and transferring what we know, the products of our research and our planning, to the grass-roots levels including local governments, families, and citizens.

We must develop a "culture of preparedness" beginning at the grade school level as well as in new university curricula related to homeland security and infrastructure assurance. We need to enhance education outreach through town meetings and community exercises. The approach can be generalized and universities are in an excellent position to lead.

3 Preparedness approaches are needed that encompass both natural hazards and malicious hazards.

One of the major lessons from our Katrina experience is that homeland security solutions involve more than dealing with terrorism and malevolent threats. Since the consequences of natural and malicious insults are similar, we can approach risk management to both classes of hazards in a similar way.

4 It is helpful to view critical infrastructure as a "commons."

We need to look beyond market forces in our planning since critical infrastructure is something from which we all take, we all ought to give back. We need to protect and manage these "commons" so the benefits are sustained. This means we need to demand strategic investments in infrastructure assurance.

Many of the critical infrastructure sectors have, in fact, solved their own problems reasonably well. For example, the banking system is well-positioned to deal with catastrophic failures. What hasn't happened is widespread transference of vulnerability and response information from the sectors that have done better. The problem is exacerbated by current industry practices in which we rely totally on the market to work out its own issues. Current business practices that look to the market to provide all solutions, have led to such things as very lean organizations, capacity shedding, just-in-time deliveries, and outsourcing which seriously increase system vulnerability. The fact of matter is that a marketing solution for the banking industry may not be the best solution for the nation as a whole. Until the government at the national level steps up to say that there are higher level objectives other than market forces across sectors, the situation will not improve. Because the individual sectors are maximizing their own business utility functions for themselves, the "commons" is not being managed.

We must not assume we will not make the same mistakes as earlier societies. We can learn from the mistakes of history. We must also not discount their solutions. Given the vulnerability of our electronic controlled systems, we may find that some solutions involve using older, simpler, more physically robust technologies and in the lifestyle that preceded our modern complex technology-driven culture. Not all preparations need to be complex.

5 Planning is crucial in the context of "Evidence-based disaster planning." Contrary to what has happened in the past, we must base disaster plans on what people are likely to do, rather than what they should do.

Since it is not possible to prevent all attacks, we need to plan to mitigate their effects. Notwithstanding our inability to predict catastrophic event onset and effects, there are some themes that run through every disaster. It is possible to predict recurring problems and the behaviors of people during those times.

We find that people can and do behave altruistically. But we need to recognize that individual plans often collide. Thus, what appears to be "panic" is, in reality, something that is better thought of as "planic." Social scientists are correct in asserting that we shouldn't call this panic. It is often the result of the problem of too much detail. A surplus of information can actually be

counterproductive and lead to paralysis.
A new area in medicine and in emergency response in particular is called "evidence-based disaster planning." Disaster situations always involve overwhelming numbers of victims arriving at treatment centers in a short time while little information is available regarding the hazard.

First responders include state officials and federal resources. But we need to work our way down in the other direction to the public. The public is an important responder. Field experience illustrates this point again and again. One of the many assumptions made in disaster planning is that trained emergency personnel will triage people in the field. But reality dictates that people aren't going to wait. What really happens is that disaster survivors, most often ordinary citizens, carry out their own search and rescue, their own triage, and, whether they recognize it or not, a lot of the primary medical care.

In wake of Katrina there has been a shift in emphasis in planning to "respond and recover" – but we need to balance this with protection/prevention. Most of the damage in New Orleans was due to flooding caused by inadequate protective walls. In the development of systems, first order empirical data indicates that the growth in the cost of fixing defects is almost exponential across the development life cycle. So obviously, the sooner a problem is recognized, the wider the range of available options. We should avoid trying to solve the problem by using patches once failures start occurring. It is thus important to include catastrophic event preparedness as an organic part of community and system planning.

6 We need to plan for a class of national scale disasters that pose a significantly greater challenge than local or even regional disasters such as Hurricane Katrina.

Examples include nuclear EMP and national-scale epidemics. Such national scale disasters deserve particular attention to preparedness and recovery since assistance from non-affected regions of the nation could be scarce or nonexistent. A major problem with such disasters is maintaining communication and transportation line connectivity. Communities and regions become isolated making it difficult to sustain their survival. Other types of national scale disasters include disease epidemics and direct nuclear attack.

Infrastructure networks are all "N minus one" (N-1) systems which are designed to operate assuming only one site in the network will fail at a time. The operators know how to recover if one system fails. They are high reliability systems and only one or a few backup systems are kept on hand. However if you have a failure of a large number of systems (in some scenarios, closer to N system failures) rather than just one, operators rarely have experience recovering from this situation.

We presently don't have the ability to analyze large scale failure modes. Some simple models show that cascading failures sometimes turn around, but sometimes keep growing, yielding infrastructure service availabilities asymptotic to zero. Such situations, if true, would make recovery very difficult. We need to develop modeling capabilities capable of analyzing complex, interconnected infrastructure failure and recovery, including failures that occur simultaneously throughout the infrastructure.

A non-trivial problem is monitoring wide-scale effects to infrastructure networks. The status of the infrastructure is reported back through communications lines that are, themselves, vulnerable. The power blackout of 2003 illustrated the problem – operators did not have information on wide-scale system status, i.e. which transmission lines were still functional. We need to protect the system status-monitoring systems so we know what's happened and how to respond and recover. It will be important to red team this. We shouldn't assume the people responsible are going to do it, or even know how to do it.

7 Assessments are a very important part of grass-roots efforts.

Assessments enable an in-depth understanding of what's out there, and how the systems work and interrelate. In many cases, local public works departments don't have a full grasp of their system operation, network geography and interconnections. Assessments also reveal how systems may fail and the full range of consequences of those failures. And assessments reveal ways to improve system resiliency through design changes or work-around procedures.

DHS is implementing a risk-based allocation formula, recognizing we can't protect everything. There are thousands of critical facilities nationally. Assessments are an essential part of this strategy. Risk assessment involves evaluating system criticality, operative threats, and system vulnerability. There is an implied division of responsibility. Criticality must be defined by the private sector and the government. The threat must be defined by the government. Infrastructure service providers must be involved in determining vulnerability. The magnitude of the challenge will require the involvement of local agents as part of regional government/industry/academic consortia. There is a critical need for local assessment criteria, goals and metrics.

People automatically assume that system protection is going to be very expensive. It doesn't come free, but a lot of the most effective fixes that have been implemented on DoD facilities have been low cost procedural fixes. Relatively low-cost steps such as adding or repositioning fences, changing car and foot traffic patterns, blocking windows into critical equipment rooms, and removing exploitable information from websites greatly improved security at critical military sites.

8 The "human infrastructure" is all important in prevention/ protection/ response/ recovery strategies.

In our planning, we must include humans as a critical infrastructure. This heightens the awareness that communities and organizations, as complex systems, require specific attention to protect them against disruptive events.

Continuity of operations planning (COOP) is essentially important because it integrates the role of human infrastructure into the preparedness and recovery process. COOP provides a very useful framework. COOP involves organizations individually and collectively identifying their essential functions that must be sustained in the event of a given catastrophe. Organizations also identify their essential personnel along with the equipment needed to enable essential personnel to execute their functions. Vital records must be identified. COOP planning enables organizations to know clearly, before an event, what needs to be done, how it needs to be accomplished, and by whom. COOP planning must start at the community level.

Viewing humans as a critical infrastructure points to human psychology as an important consideration relative to infrastructure assurance. People at the grass-roots are psychological resources. These grass-roots resources include parents, citizens, teachers, clergy, and volunteers who have opportunities to assist individuals hit by a natural disaster or an act of terrorism. During times of crisis, it is helpful to recognize that affected individuals are not victims – they are survivors.

The human infrastructure is inherently resilient and adaptable and this resilience can be greatly enhanced by the proper approach. In terms of an infrastructure (including technology and businesses, economics, and so forth) psychologists are quite interested in the personal resilience – the psychological resilience of individuals.

It is also helpful to look at our human infrastructure as a "commons" in developing a psychological sense of community. In this regard, the new field of "positive psychology" holds promise. Psychologists are realizing the importance of looking at the whole human experience… not just the problems. This "positive psychology" includes attention to human strengths, character, and resilience. Positive psychology has been an important influence in the field of crisis intervention. We are beginning to look at individuals in crisis situations not as passive, pathetic victims who are dealing with communities that are totally destroyed; but rather to see them instead as having possibilities, potential and strengths that we can use to enable them and facilitate a resolution process. This leads to the concept of personal and community resilience, analogous to physical infrastructure.

Steps in human infrastructure recovery include community support, meaning making, managing emotions and actions to restore the future. The greater the physical and emotional support environment, the more people are able to come through the event at a higher level of well-being. A principled, "devictimizing" strategy is important.

Organization of the Symposium

The Symposium was a one day event organized around four panels addressing "Prevention," "Protection," "Response," and "Future Horizons." Lynda Stanley, Director of the Board on Infrastructure and the Constructed Environment, National Research Council, opened the Symposium. Dr. John Noftsinger, Vice President for Research and Public Service, James Madison University provided an overview of the days events. The opening address was delivered by Dr. Linwood Rose, President of James Madison University. Featured speakers on selected current topics were included before and after each panel.

7:30-8 am Continental Breakfast and Networking

8:00-8:05 Welcome to the National Academies – Lynda Stanley, Director, Board on Infrastructure and the Constructed Environment, National Research Council

8:05-8:15 Welcome and Symposium Introduction – Dr. John Noftsinger, Associate Vice President for Research & Public Service at James Madison University and Executive Director, Institute for Infrastructure and Information Assurance (IIIA), and Dr. Douglas T. Brown, Provost and Vice President for Academic Affairs, James Madison University

8:15-8:45 Opening Address – Dr. Linwood Rose, President of James Madison University and Member of the National Infrastructure Advisory Council (NIAC)

8:45-9:15 Featured Speaker – Dr. William R. Graham, Science Advisor to President Reagan …*On infrastructure protection on a national scale.*

9:20-10:25 Prevention Panel Discussion
Issues: How are we doing on preventing infrastructure attacks? How well is the national strategy working? What's not working? How can we improve our efforts with special attention to engaging the grass-roots?
Panelists: Mr. Fenton "Dutch" Thomas, MSA Incorporated (Panel Moderator) – National Preparedness; Mr. Taz Daughtrey, James Madison University, IIIA Associate Director for Software Development – Cyber Security and Risk Assessment; Mr. Richard Little, University of Southern California, Director, Keston Institute for Infrastructure – Critical Infrastructure Protection; Mr. David Moore, National Security Agency – Cognitive Solutions Dr. Peter Pham, James Madison University, Director of the Nelson Institute for International and Public Affairs – Diplomatic Solutions

10:30-10:45 Morning Break

10:45-11:15 Featured Speaker – Mr. Daniel W. Caprio, Jr., The Progress & Freedom Foundation, Senior Fellow and Executive Vice President *…On RFID developments*

11:20-12:25 Protection Panel Discussion
Issues: How well are we protecting infrastructure? Which models and experiences showcase what is working and what's not working? How can we improve our efforts?
Panelists: Mr. Patrick Bridge, Virginia Department of Health (Panel Moderator) – Regional Emergency Preparedness and Response; Dr. George Baker, James Madison University, IIIA Associate Director for Infrastructure Research – Infrastructure Assessment; Dr. Jerry Brashear, American Society of Mechanical Engineers – Protection Standards; Dr. Ronald Raab, James Madison University – Vaccine Development; Dr. Eric Tollar, SAIC, Senior Analyst for Radiological and Nuclear Countermeasures – System Analysis and Protection

12:30-1:25 Lunch and JMU Research Poster Session in the Great Hall

1:25-1:55 Featured Speaker – Mr. Michael Lowder, FEMA Deputy Director for Emergency Response… *On national disaster response programs*

2:00-3:00 Response Panel Discussion
Issues: How are we doing vis-à-vis response planning and implementation? Which collaborations are facilitating efforts to engage grass-roots infrastructure?
Panelists: Ken Newbold, James Madison University (Panel Moderator) – Secure Software; Mr. Joshua Barnes, MSA Incorporated – Continuity of Operations; Dr. Lennie Echterling, James Madison University – Disaster Psychology; Dr. Mark Kirk, University of Virginia – Emergency Medicine and Situational Management; Dr. Greg Saathoff, University of Virginia – Community Shielding

3:00-3:10 Afternoon Break

3:15-4:15 Future Horizons for Infrastructure Protection
Issues: New ideas and approaches for engaging the frontlines.
Panelists: Dr. John Noftsinger, James Madison University, AVP Research & Public Service and Executive Director, IIIA (Panel Moderator) – Partnerships; Mr. Frank J. Cilluffo, The George Washington University, Associate Vice President for Homeland Security and Director, Homeland Security Policy Institute – Policy Solutions; Dr. Noel Hendrickson, James Madison University – Critical Thinking Skills for the Intelligence Community; Dr. Newton Howard, The Center for Advanced Defense Studies, Founder and Chairman – Digital Defense

4:20-4:40 Keynote Address – Mr. John A. McCarthy, George Mason University, Director and Principal Investigator, Critical Infrastructure Protection Project … *On private-public partnerships.*

4:40-5:00 Q&A for the Day and Closing Remarks – Dr. Jerry Benson, James Madison University, Dean, College of Integrated Science & Technology, and Mr. Steve Knickrehm, James Madison University, IIIA Associate Director for Policy

Welcome

Lynda Stanley, Director, Board on Infrastructure and the Constructed Environment, National Academies

Ms. Stanley welcomed attendees on behalf of the Board and the Federal Facilities Council. She encouraged participants to take advantage of the many notable experts on infrastructure assurance in the room and make it a point to converse and get some new perspectives and ideas. She explained that the National Academies consists of four different organizations including National Academy of Sciences, the National Academy of Engineering, the Institute of Medicine, and the National Research Council. These can be thought of as the same group for most purposes.

The charter of the National Academies is to provide objective, independent advice to the government, the public, the scientific and the engineering communities on issues related to science and technology. The National Academies, a Congressionally chartered, private, non-profit organization, was especially set up by Abraham Lincoln in 1863 to provide objective, independent advice. That is still the mission. The National Academies is not a government agency.

The Board on Infrastructure and the Constructed Environment is the Academy organization that addresses questions of science, technology and public policy as they relate to the constructed environment both above and below ground. Two major activities that we have are the Federal Facilities Council and the Critical Infrastructure Roundtable. The Federal Facilities Council itself is 26 separate federal agencies that pool their resources to do activities that will benefit all agencies. The National Academies provides neutral ground for this consortium. The mission is to identify and advance technologies and processes to essentially make federal facilities better over their entire life cycle, from planning to disposal of the facilities. The objective is to get the best return on taxpayer dollars.

One of the key areas the Federal Facilities Council addresses is physical security. As a group we have published quite a few studies on security and physical protection going back to the 1980s when we were looking at federal buildings and how to protect them from bomb damage. More recent studies have dealt with building design criteria. The National Research Council has conducted benchmark studies on protective design approaches for the Federal facilities Council (1984), US Department of State (1986), Defense Nuclear Agency (1993), the Defense Threat Reduction Agency (2001), and the General Services Administration/Dept of State/Administrative Offices of the US Courts (2002). These studies are posted on our National Academy Press website, www.nap.edu. There are 50-60 studies on security available.

Welcome

John Noftsinger, Associate Vice President for Research and Public Service, James Madison University, and Executive Director for the Institute for Infrastructure and Information Assurance

Dr. Noftsinger welcomed attendees on behalf of James Madison University and the Institute for Infrastructure and Information Assurance (IIIA) which he directs. He thanked the National Academies of Science and our host, Lynda Stanley.

An important lesson can be learned from the establishment of the National Academies during the Civil War. One can imagine the travail of the civil war and the stress that Abraham Lincoln must have felt during those days. If you have studied Lincoln, you know the struggles he had personally and emotionally as a leader. Certainly our nation was torn at that time. The United States is experiencing similar challenges today – maybe not on that magnitude. During that time of national crisis, Lincoln had the foresight to look to science and establish in 1863 the National Academies. His vision can inspire us today.

The IIIA at JMU is our center for homeland security-related research. We focus on the unique intersections of infrastructure and information assurance and both physical and cyber protection. We are pleased to be partnering with George Mason University on the Critical Infrastructure Protection Program (CIPP). Under the leadership of Congressman Frank Wolf, we established this program in 2002, however, the actual conceptualization of the program occurred September 11, 2001. I would like to express special thanks to George Mason University, who will be represented in the program today and to Congressman Wolf for his leadership.

The Homeland Security endeavor necessitates a strong role for collaboration among government, academia, the private sector, and nonprofit organizations. We hope this event will foster dialogue and connections among you that lead to improved collaboration. Specifically, it is my hope that we will leave this room and follow up on connections and ideas that form here.

The IIIA has just established a Fellows Program to recognize outstanding individuals who have made substantial contributions to the homeland security endeavor. Today we recognize the first class of fellows: Dr. Lenny Echterling and Dr. Peter Pham. For our first class of fellows we looked within our university. In the future we hope to tap leaders both inside and outside JMU.

Dr. Lennis G. Echterling
James Madison University
Director of Counseling Psychology. Crisis intervention, Resilience and Thriving, Disasters and Terrorism

2007 IIIA Fellow, Dr. Echterling serves as a professor of graduate psychology at JMU. He directs the counseling psychology research program. He has more than 30 years of experience in crisis and disaster psychology. His research interests include: crisis intervention, disaster psychology, terrorism, and especially the area of resilience. His books include Crisis Intervention, Promoting Resilience and Resolution in Troubled Times, Ideas and Tools for Grief Counseling, and Thriving! A manual for Students in the Helping Professions. Dr. Echterling has received James Madison University's Distinguished Faculty Award, Virginia Counselors Association's Humanitarian and Caring Person Award, and the National Counseling Vision and Innovation Award from the Association for Counselor Education and Supervision. He served as a disaster outreach volunteer when tornadoes impacted the Midwest. He's helped design programs to help communities respond to disasters. For over 20 years he has volunteered with a program supporting firefighters, rescue workers, law enforcement organizations. Following the tragic events of September 2001, Dr. Echterling volunteered with the Red Cross at the Pentagon, and has most recently provided disaster counseling and intervention for Mississippi and Texas in the wake of the Katrina and Rita hurricane disasters.

2007 IIIA Fellow, Dr. J. Peter Pham is Director of the William R. Nelson Institute for International and Public Affairs and assistant professor of justice studies at James Madison University. Among other academic qualifications, he holds graduate degrees in international affairs, administrative law, and international law as well as theology and canon law. His research interests are at the intersection of international relations, international law, political theory and ethics with particular concentrations on implications for United States foreign policy and African states as well as religion and global politics. During the current academic year, he is directing a pilot study on Africa's place in a strategic vision of America's future energy security. Peter is the author of over one hundred essays and reviews on a wide variety of subjects in scholarly and opinion journals on both

Dr. J. Peter Pham
James Madison University
Assistant Professor of Justice Studies; Director, Nelson Institute for International and Public Affairs

sides of the Atlantic. He is the author, editor, or translator of over a dozen books. He is the recipient of a 2005-2006 Academic Fellowship on Terrorism from the Foundation for the Defense of Democracies. He is presently completing a major study on terrorism in Sub-Saharan Africa. Prior to his appointment at James Madison University, Dr. Pham served as an international diplomat in Liberia, Sierra Leone, and Guinea from 2001-2002 and was selected to serve as an official U.S. delegate to monitor the Liberian national elections in October 2005.

Welcome

Dr. Douglas Brown, Provost, James Madison University

Dr. Doug Brown added his welcome and introduced the first keynote speaker, Dr. Linwood Rose. Dr. Rose is the fifth president of James Madison University, having served at a time in the university's history when we have experienced the greatest growth and diversification of our programs ever. He has shepherded the university to a position of national prominence in which we have engaged in a very deliberate way in science, technology, homeland security, information security and infrastructure protection. In doing this we have involved a large range of disciplines in addition to science and technology to include the health profession and business, working at local, state, and national levels. Dr. Rose facilitated the development of the Critical Infrastructure Protection Program. He provided the initial leadership in forming the IIIA which is co-hosting today's symposium. He has secured funding for CIP projects within the Commonwealth of Virginia. He was appointed by President George W. Bush as the only academic representative to the National Infrastructure Advisory Council where he continues to serve.

Opening Address:

Dr. Linwood Rose, President, James Madison University

I'd like to provide a slight disclaimer. I'm here today as the President of my institution, not as a member of the NIAC nor any other board or advisory council. I don't come today to you as a computer scientist, an engineer, as a health official, or as a city planner, but as President of an institution that has as part of its mission the development of educated and enlightened citizens.

I mention this because that phrase could easily say educated and enlightened people. But our institution focuses on the development of citizens. I lead a university in which civic engagement, service, and outreach represent not activities, but values. While I believe we have much to offer, it is the sharing of our individual and collective expertise in the context of these values that sets us apart.

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

Given the location of this meeting, it is probably safe to assume that many of you have sons or daughters who attend James Madison University. And if you're a parent of an applicant for this coming fall I hope that your son or daughter was admitted. With over 20,700 applicants for admission this year and 3,700 openings, I'm afraid we disappoint many more hopeful applicants than we please. We will enroll approximately 17,000 students this coming fall.

As has been mentioned, this is the fourth annual symposium and JMU is delighted to host this one in cooperation with the Federal Facilities Council. And we are particularly pleased to hold it at this location. It is the first time we've hosted the symposium in the Washington, DC area and I want to add my thanks to the Academies and the Federal Facilities Council. I also add my welcome to each of you this morning. It's great to see such a wonderful turnout and representatives from so many organizations. We are delighted by the overwhelming response. My thanks to all those who worked behind the scenes to make this day happen and we appreciate all your efforts. Thanks to you who are giving presentations or who have agreed to serve on a panel. We appreciate your making time to share your expertise with us today. We look forward to some great discussions throughout the day.

College and university presidents are often on the road as much as they are in their own offices. We promote our institutions. We constantly strive to promote new relationships. We solicit funds. We share the myriad ways our faculty, our staff, and yes, our students contribute to the common good and the betterment of our way of life. I'd like to mention in passing some information about the university's ratings. We were again number one in the *US News and World Report* as a comprehensive public university in the South. We were recently ranked by *Kiplinger's Magazine* as the 17th best value in the country among all public universities in the United States. And we are ranked by *Newsweek Magazine* as the 35th best undergraduate business school in the country.

Throughout history, American universities have served as catalysts for change. And the university research laboratory has been the birthplace of many life-changing discoveries.

Let me say a few words about why we're here today. The Symposium is designed to share information on topics of research related to DHS, including protection, prevention, and response. It is also an opportunity to discuss opportunities for the future – what more we need to do. But, just as important, today is a unique opportunity to talk with each other. We designed this symposium with this in mind – to bring us together for discussion of common issues and common concerns. We represent different sectors: government, education, and industry. For most of us, our paths don't cross as often as they might. We need to work together more. And when I say "we" for education, I don't just mean within Virginia. We have a number of universities present today from other states. We have the opportunity to explore issues together – to view them from multiple perspectives and to discover where our roles intersect and overlap. I hope that when we leave here today, we can better envision how we can collaborate to address issues of Homeland Security.

At the national and state levels we tend to view physical, chemical, biological, and cyber issues of homeland security from a perspective at 10,000 feet. But transferring what we know, the products of our research and our planning to the grass-roots levels – to local governments, families, and citizens – can be a complicated challenge. Some of the university's research and publications specifically address local community and family security and response strategies such as our risk assessment modeling software and our citizens guides for emergency preparedness. I hope that our symposium discussions will include these elements of homeland security.

I'd like to speak to the topic of university research for a moment. I believe that university research is absolutely essential to finding solutions to many of the issues that we face. Throughout history, American universities have served as catalysts for change. And the university research laboratory has been the birthplace of many life-changing discoveries – everything from new medical breakthroughs, improved transportation, sustainable agriculture, renewable energy, to information security, to name just a few.

While university research has boomed over the last half century, universities are becoming more strategic about the integral role that they play in using their expertise to address societal issues as they develop institutional missions. For instance, the Kellogg Commission was created to define the direction public universities should go in the twenty-first century and recommend an action agenda to get there. The Commission described public universities as "engines of discovery that have helped the people of the United States and frequently the world to deal with the intractable problems before them." In looking toward the future, the Commission called for renewed commitment among public universities to conduct research and to engage directly with society and its problems and all in the service of advancing the common good.

In that same vein, earlier this year, in its Winter 2006 issue, of *Presidency Magazine*, the American Council on Higher Education announced "Solutions for Our Future – A New Campaign." Part of this campaign is educating the American public about the ways universities create opportunities and find solutions. To quote David Ward, President of the American Council on Higher Education, "Our colleges and universities contribute to the economy, well-being and quality of life in our country. They provide people, ideas, and scientific and technical advancements that will be sources of solutions for society's most pressing problems." I concur with Dr. Ward's assessment. Some of the greatest minds in the world are found in the university research laboratory and classroom, and many are represented here today. Now don't misunderstand me. I am certainly not suggesting that universities have a corner on great minds. My comment isn't rooted in intellectual snobbery, elitism, or arrogance – but rather a desire to fully engage and take advantage of one of our nation's greatest resources. It is absolutely imperative that we develop ways to enable these great minds to make the next discovery. They need the tools to explore and research. We need to find ways to get that information out of the laboratory and into the hands of people who need it and will benefit from it. Just this week, the *Chronicle of Higher Education* reported that while overall research and development spending at colleges increased by 7.2 percent to $42.9 billion, industry support of university science and technology research fell for the third year in a row to $2.1 billion. We need to better understand the causes of this trend. Perhaps through our interaction today we can learn more.

We designed this symposium with this in mind – to bring us together for discussion of common issues and common concerns.

Although it is but one aspect of homeland security, cyber security is a personal interest of mine. And while obviously biased, I believe we have some very talented folks working in this area at JMU. We recognized in the late 1990s that more information security professionals were needed in both the public and private sectors and we introduced a masters degree in information security. That program, intended for working professionals, was at the time- and may still be- the only such degree program in the nation provided to students via the internet. Approximately one-half of our students are from government. The remaining participants come from industry. I expect we have some graduates with us today. We have also developed instructional curricula in secure software design and have begun development of a unique curriculum for information analysts.

Let me turn my attention to information security research. In the face of natural disasters, and a literal war on terrorism, it's understandable that federal, state, and corporate resources are skewed toward addressing those issues. Protecting the physical infrastructure is critically important. No one doubts it. However, I am concerned that cyber security research is inadequately funded, driven by short-term, immediate needs, and suffers from a lack of focus and prioritization. The National Security Agency has championed college and university efforts in cyber security education and research. The National Security Foundation has provided the bulk of funding to higher education in this area, which we most appreciate.

Concerns have been expressed about the adequacy of the cyber research talent pool. My own opinion is that a sufficient number of computer scientists, engineers, and experts from other disciplines will gravitate to cyber research if support is adequate, sustained, and predictable. While security clearances and proprietary restrictions are always an issue in this research area, I believe cyber security research is a fertile area for collaborative university, government and private sector efforts.

At JMU, the Institute for Infrastructure and Information Assurance was created in 2002. It was created to serve as a vehicle to address homeland security and national defense interests. The institute is conducting research in a number of areas including assessment and modeling, prevention, protection, response and education. We look forward to sharing some of that research today through our panel discussions. The IIIA serves as a model for collaboration. It has funded over 40 research projects at JMU and other Virginia universities, and has developed creative and innovative partnering relationships with industry and government agencies. Partnerships include George Mason University, University of Virginia, Virginia's Institute for Defense and Homeland Security, the Virginia Information Technology Agency, the Center for Innovative Technology, the National Park Service, and numerous private sector organizations. The institute also provides a unique and valuable experience for JMU students. Its work appeals to students who are always looking for relevancy and opportunities to solve hard problems that matter. IIIA also provides professional development opportunities for our faculty. IIIA was one of the founding members of VA SCAN – the Virginia Alliance for Secure Computing and Networking and has helped sponsor computer security education and training for IT professionals.

> *Dr. Graham's talk provides a global perspective on infrastructure assurance using the EMP threat as an example of a national scale disaster consequences and preparedness.*

I want to thank you again for joining us today. I've tried to provide a brief overview of JMU and IIIA and set up some objectives for the day. We look forward to your active engagement throughout the day.

Introduction

Dr. George Baker, Associate Director for Infrastructure Research, Institute for Infrastructure and Information Assurance

Dr. Baker introduced Dr. William Graham – Dr. Graham has a very distinguished career at the forefront of America's science and technology development and policy and has served in many national leadership roles in ballistic missile defense, space exploration, arms control and disarmament. During the Reagan Administration he directed the White House Office of Science and Technology Policy as well as serving as President Reagan's Chief Science Advisor at a time in our history where the assertion of U.S. technology capabilities was instrumental in ending the Cold War. He was a 2005 Visiting Scholar at James Madison University. He has just been reappointed as Chairman of the Congressional Committee to Assess the Threat to the United States from the Nuclear Electromagnetic Pulse. Dr. Graham's topic stems from this Chairmanship. Dr. Graham's talk provides a global perspective on infrastructure assurance using the EMP threat as an example of a national scale disaster consequences and preparedness.

Featured Speaker

Dr. William Graham, Chairman, Congressional Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack.

Some have likened commissions to a fourth branch of government. There are permanent commissions that you are aware of such as the Nuclear Regulatory Commission and the Security and Exchange Commission. There are also many ad hoc commissions. These include commissions on almost any subject you can imagine: tax reform, education reform, and 9-11. Dr. Graham chairs an ad hoc commission on the threat to the US from a wide-area nuclear weapons phenomenon that would occur if a nuclear weapon were detonated high above the homeland. His talk relates this to a more general set of infrastructure protection issues. EMP represents an important class of large-scale infrastructure assurance problems.

EMP results from a nuclear weapon detonated at altitudes ranging from about 40km to many hundreds of kilometers. In the cold war we were worried about the effects of large-scale direct attacks on the continental United States in the hundreds to thousands of nuclear warheads which would physically destroy most of our infrastructure. We hope we're in a different era now. But even a few nuclear weapons, even one or two, can cause an effect that involves issues characteristic of the larger class of national scale infrastructure attacks.

When the Soviet Union conducted exoatmospheric nuclear tests back around 1960 we suspected that they had discovered the same effect of which we later learned. And, in fact, after the cold war, when Soviet nuclear scientists began appearing at international symposia, they started talking about it. The following chart is a translation of a chart in Russian presented by General Loborev. It depicts power and communication systems that failed underneath their high altitude detonations which they conducted over large land masses. See Figure 1

We recognized the phenomena depicted in this chart because we had conducted a test somewhat similar to this but over the Pacific Ocean in 1962. Our "Fish Bowl Series" was the second and last U.S. high altitude nuclear weapons test series. One of the tests in this series, the "Star Fish" test, involved detonating a megaton-class weapon at 400km over Johnston Island. That altitude put the burst just above the horizon of Owahu. Simultaneous with this detonation a number of strange things happened in Honolulu. In particular, many strings of the Honolulu street lights failed. Burglar alarms and other alarms went off. Communication links, particularly microwave links, failed exactly at the detonation time. We know this because we were using microwave links to provide timing signals for our nuclear test measurement instrumentation systems. Because of the instantaneous, wide scale effects, we suspected something electromagnetic had happened but we didn't understand what.

The study of EMP had begun with Enrico Fermi in the first U.S. nuclear weapon test, "Trinity." He predicted that there would be some electromagnetic effects from nuclear weapons. Evidence of such effects was provided in early tests by errors noted on measurement traces. Strong fields from nuclear weapons interfered with recording equipment, causing oscilloscope traces that looked like balls of yarn. But this effect that could take out street lights at very large distances was initially not understood.

In the fall of 1962, I arrived at the Air Force Weapons Laboratory as a fresh Ph.D. Since the Air Force didn't understand much of the data they'd collected they decided to get a lot of new minds to work on the problem. They assembled a group of fresh Ph.D.s and asked them to look at the data and explain what was causing electrical equipment failure and erroneous instrument readings. The team leaders reached out for help from a noted plasma physicist at Los Alamos by the name of Conrad Longmire. Longmire was asked to give a series of lectures on nuclear electromagnetic effects. In the process he was able to develop the theory to explain this phenomenon.

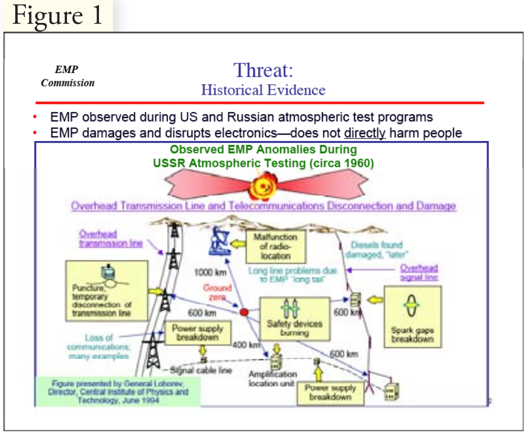
Those of you in academia know there is nothing as inspiring as a problem that you have to explain to the class the next day. That was the problem that faced Longmire. Sitting by a swimming pool at Los Alamos, he actually worked out the theory of the large amplitude high altitude EMP. In a flash of insight, he figured out that the combination of the gamma rays coming out of the bomb, interacting with air atoms by stripping off "Compton" electrons, the electrons traveling outward synchronously at the speed of light, produced an intense, pulsed electromagnetic field. The Compton electrons, turning coherently by the earth's magnetic field, create a huge phased array transverse current antenna in the sky. Any area on the earth's surface within line-of-sight to the nuclear explosion will experience an electromagnetic signal radiated by this transverse current.

It's an amazing thing. The gammas come out in the first 10 nanoseconds creating a 10 foot thick shell of gamma photons that remain coherent out to more than 1000 kilometers. This produces, in effect, a huge antenna that radiates downward. Depending on the characteristics of the weapon, the amplitude of the radiated electric field ranges from a few kilovolts per meter to possibly more than 100 kilovolts per meter with a rise time of 10 nanoseconds. Longmire's original theory proved to be correct.

Unfortunately we're not the only ones who know about this. Over the last decade, awareness has spread around the world to countries that are developing nuclear capabilities. As an example, the following chart provides some quotes from Iranian publications: See Figure 2

It's interesting to note the last bullet. The Iranians have test launched a Scud missile from a surface vessel. The launching occurred during a test in the Caspian Sea. This launch mode could support a national or trans-national terrorist EMP attack against the United States. Scud missiles are readily available around the world. There are thousands of them around. They're being shipped into the US to arms collectors. Although they are fairly short range, the missiles are capable of lofting a nuclear weapon to a 100 km

Figure 1



EMP Commission

Threat:
Historical Evidence

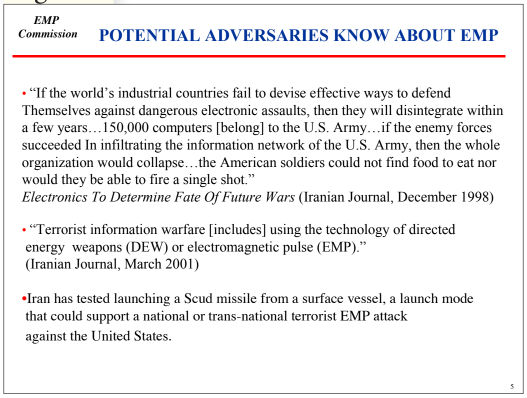
- EMP observed during US and Russian atmospheric test programs
- EMP damages and disrupts electronics—does not directly harm people

Observed EMP Anomalies During
USSR Atmospheric Testing (circa 1960)

Overhead Transmission Line and Telecommunications Disconnection and Damage
Overhead transmission line
Malfunction of radio-location
Diesels found damaged, "later"
Overhead signal line
1000 km
Long line problems due to EMP "long tail"
Puncture, temporary disconnection of transmission line
Ground zero
600 km
Safety devices burning
600 km
Spark gaps breakdown
Power supply breakdown
400 km
600 km
Loss of communications; many examples
Signal cable line
Amplification location unit
Power supply breakdown

Figure presented by General Loborev, Director, Central Institute of Physics and Technology, June 1994

Figure 2



EMP Commission

POTENTIAL ADVERSARIES KNOW ABOUT EMP

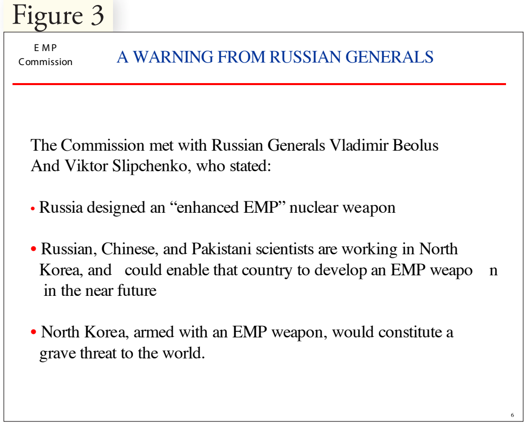
- "If the world's industrial countries fail to devise effective ways to defend Themselves against dangerous electronic assaults, then they will disintegrate within a few years…150,000 computers [belong] to the U.S. Army…if the enemy forces succeeded In infiltrating the information network of the U.S. Army, then the whole organization would collapse…the American soldiers could not find food to eat nor would they be able to fire a single shot."
Electronics To Determine Fate Of Future Wars (Iranian Journal, December 1998)

- "Terrorist information warfare [includes] using the technology of directed energy weapons (DEW) or electromagnetic pulse (EMP)."
(Iranian Journal, March 2001)

- Iran has tested launching a Scud missile from a surface vessel, a launch mode that could support a national or trans-national terrorist EMP attack against the United States.

5

Figure 3



EMP Commission

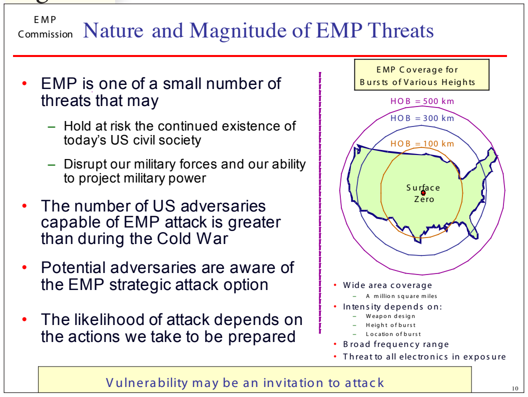
A WARNING FROM RUSSIAN GENERALS

The Commission met with Russian Generals Vladimir Beolus And Viktor Slipchenko, who stated:

- Russia designed an "enhanced EMP" nuclear weapon
- Russian, Chinese, and Pakistani scientists are working in North Korea, and could enable that country to develop an EMP weapo n in the near future
- North Korea, armed with an EMP weapon, would constitute a grave threat to the world.

6

Figure 4



EMP Commission Nature and Magnitude of EMP Threats

- EMP is one of a small number of threats that may
  - Hold at risk the continued existence of today's US civil society
  - Disrupt our military forces and our ability to project military power
- The number of US adversaries capable of EMP attack is greater than during the Cold War
- Potential adversaries are aware of the EMP strategic attack option
- The likelihood of attack depends on the actions we take to be prepared

EMP Coverage for Bursts of Various Heights

- Wide area coverage
  - A million square miles
- Intensity depends on:
  - Weapon design
  - Height of burst
  - Location of burst
- Broad frequency range
- Threat to all electronics in exposure

Vulnerability may be an invitation to attack

10

altitude, sufficient to create EMP over large regions of the US – even if launched off-shore.

It is not just the Iranians who are interested. The EMP Commission, just re-established by Congress, has been talking with Russian generals Vladimir Beolus and Viktor Slipchenko. Some of their pointed comments are included in the following chart:

See Figure 3

As a commission we were asked to look forward 15 years to see what we could say about the vulnerability of military, and especially civilian systems in the U.S., and what we might be able to do about it before and after a potential nuclear attack. The next chart shows the nature and magnitude of the EMP threat within the next 15 years.

If you detonate a nuclear weapon over the point labeled "surface zero," See Figure 4 EMP fields will reach out to the horizon as shown by the circles on the map. A scud just off one of the coasts could cover the entire coastal region. A larger missile could cover the whole country if detonated over the central part of the country. Although EMP covers the entire circular area, the fields are not uniform. One of the great ironies is the peak field pattern looks like a smiley face.

We do not know how to predict the probability of an EMP attack. But the Commission did look at the capabilities of interested countries. We are convinced that within 15 years it would certainly be within the capabilities of a number of them. Secretary of Defense Rumsfeld has a favorite saying, "Vulnerability may be an invitation to attack."

With regard to vulnerability, the EMP Commission looked at the effects of EMP on a number of kinds of systems. With such a large scale event, there is the possibility of damaging the electrical and communications infrastructure over a region that scales to a significant fraction of the entire country. There aren't a lot of phenomena that threaten us on that scale. Obviously a large scale nuclear attack would. An organized attack on our infrastructure by internal malefactors is another. A pandemic would represent national scale threats either natural as in the bird flu or deliberate attack using a man made bioagent designed to be contagious and lethal. These are a class of problems that are so large that it becomes difficult to bring in help from the edge. The area that needs help grows proportional to the radius squared where the edge itself just grows proportional to the radius. The ability to get timely help into a larger and larger affected area from smaller and smaller unaffected areas becomes increasingly limited.

This happened to some degree during Hurricane Katrina. In another National Academy group I spoke with General Honore who brought the first high-level organization into the Katrina relief effort. He said it was a familiar situation to him as an Army general. He viewed Katrina as the enemy. It was a very skilled enemy. It took out his electronics and communications. It took out his road connectivity, isolating his forces and put them in a situation where it was difficult to sustain their survival. That's what a skillful enemy will do and that's what he had studied during his military career. EMP can be viewed in a similar manner.

EMP debilitates electronics and electrical systems. These are ubiquitous in our society and have become essential to the operation and maintenance of all infrastructures. The Commission tested the vulnerability of a number of representative critical infrastructure systems with modern electronic control systems illustrated in the following chart. We engaged a number of organizations in the government and private sector to do the susceptibility tests.

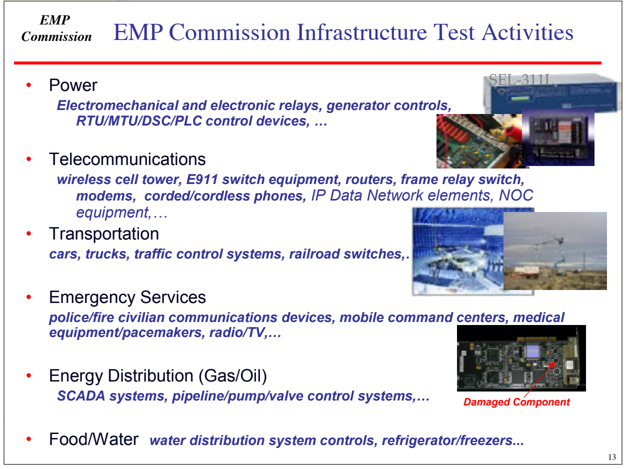
See Figure 5

We took the electric power infrastructure as our starting point. We discovered a number of potential failure mechanisms. One of the effects of a high altitude burst looks like a geomagnetic storm. These naturally occurring "solar storms" have caused outages and disruptions of large scale long distance power transmission lines. See Figure 6

The Commission determined that an EMP could bring down the national power grid. One of our commission members who was Secretary of the Interior under President Reagan had been chief engineer at the Bonneville Power Administration. In this role, he had dealt directly with recovering from large scale effects of geomagnetic storms. He pointed out that starting from a completely unpowered, "black" grid is not a normal condition. In fact, nuclear power plants which provide 20 percent of our power and provide a very reliable base load, are not designed to start into a black grid. It takes more power to start a nuclear plant than the plant has in its own backup diesel generators. The lesson is that it takes a very well thought out plan to restart a power grid once it has failed.

We also looked at telecommunications. Although we didn't look specifically at financial systems, 99% of fund-flow transactions in the United States take place electronically. If our telecommunication systems fail,

Figure 5



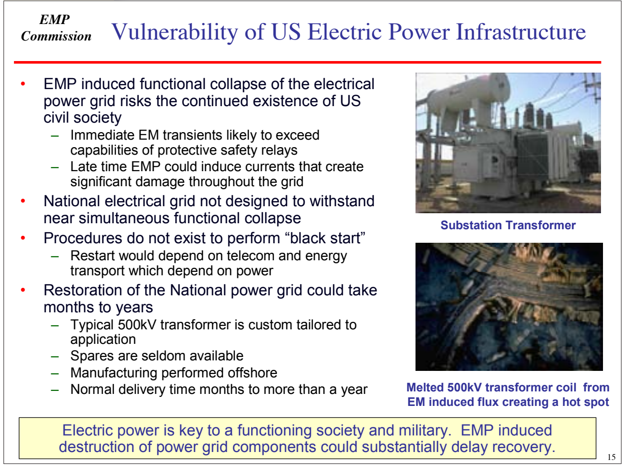
EMP Commission

EMP Commission Infrastructure Test Activities

- Power
  Electromechanical and electronic relays, generator controls, RTU/MTU/DSC/PLC control devices, …
- Telecommunications
  wireless cell tower, E911 switch equipment, routers, frame relay switch, modems, corded/cordless phones, IP Data Network elements, NOC equipment,…
- Transportation
  cars, trucks, traffic control systems, railroad switches,…
- Emergency Services
  police/fire civilian communications devices, mobile command centers, medical equipment/pacemakers, radio/TV,…
- Energy Distribution (Gas/Oil)
  SCADA systems, pipeline/pump/valve control systems,…
- Food/Water *water distribution system controls, refrigerator/freezers...*

13

Figure 6



EMP Commission

Vulnerability of US Electric Power Infrastructure

- EMP induced functional collapse of the electrical power grid risks the continued existence of US civil society
  - Immediate EM transients likely to exceed capabilities of protective safety relays
  - Late time EMP could induce currents that create significant damage throughout the grid
- National electrical grid not designed to withstand near simultaneous functional collapse
- Procedures do not exist to perform "black start"
  - Restart would depend on telecom and energy transport which depend on power
- Restoration of the National power grid could take months to years
  - Typical 500kV transformer is custom tailored to application
  - Spares are seldom available
  - Manufacturing performed offshore
  - Normal delivery time months to more than a year

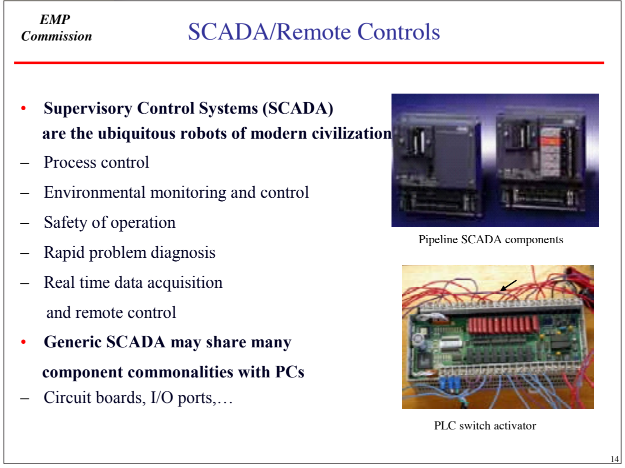
Substation Transformer

Melted 500kV transformer coil from EM induced flux creating a hot spot

Electric power is key to a functioning society and military. EMP induced destruction of power grid components could substantially delay recovery.

15

Figure 7



EMP Commission

SCADA/Remote Controls

- **Supervisory Control Systems (SCADA) are the ubiquitous robots of modern civilization**
  - Process control
  - Environmental monitoring and control
  - Safety of operation
  - Rapid problem diagnosis
  - Real time data acquisition and remote control
- **Generic SCADA may share many component commonalities with PCs**
  - Circuit boards, I/O ports,…

Pipeline SCADA components

PLC switch activator

14

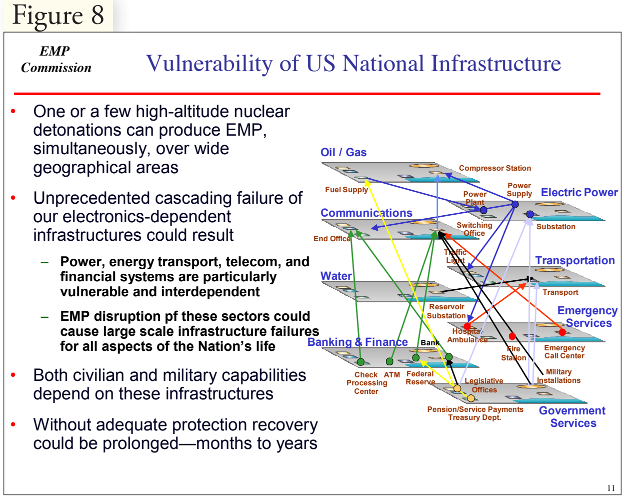
on farms and were self-sufficient with regard to food sources. Today almost no one lives on farms and we require a very complex infrastructure just to sustain life and get anything done beyond that. There is one class of electronic devices that is ubiquitous and very vulnerable to EMP. The devices are referred to as Supervisory Control and Data Acquisition Systems or "SCADA" Systems. They are basically a remote control boxes made largely out of computer components. See Figure 7

SCADA systems are not well-protected electromagnetically. They regulate the operation of most critical infrastructure systems. You can think of them as little robots present throughout our society. Our tests showed that they are highly vulnerable to EMP.

Related to the transportation infrastructure, we tested about fifty vehicles, ten of which stopped running when hit by an EMP. Nine of these ten would "reboot" and start on subsequent attempts. One car was permanently damaged and had to be towed back to the dealer to replace a computer chip. It might not sound like a lot, but the failure of 2 percent of vehicles in Washington, DC on an average business morning would completely shut down the area.

In general, we found that any electronic system that is not designed to withstand EMP, or designed against lightning or electrostatic discharge is going to be vulnerable to EMP at some level. See Figure 8

Figure 8



EMP Commission

Vulnerability of US National Infrastructure

- One or a few high-altitude nuclear detonations can produce EMP, simultaneously, over wide geographical areas
- Unprecedented cascading failure of our electronics-dependent infrastructures could result
  - **Power, energy transport, telecom, and financial systems are particularly vulnerable and interdependent**
  - **EMP disruption pf these sectors could cause large scale infrastructure failures for all aspects of the Nation's life**
- Both civilian and military capabilities depend on these infrastructures
- Without adequate protection recovery could be prolonged—months to years

The chart above depicts the grand challenge. It turns out our infrastructure systems are tightly coupled. We get the great efficiencies we have from our infrastructure because we tie them all together. We don't ask our oil and gas transmission systems to generate their own electric power. Nor do we require our banking and financial system to build their own communication systems. As you look down through the list of infrastructures it is clear they all interrelated – no infrastructure is self-sufficient.

Infrastructure networks are all what I call "N minus one" (N-1) systems which are designed to operate assuming only one site in the network will fail at a time. The operators know how to recover if one system fails. They are high reliability systems and only one or a few backup systems are kept on hand. Operators train and practice for "N-1" recovery situations. However if you have a failure of a large number of systems (in some scenarios, closer to N system failures) rather than just one, operators have no experience recovering from this situation. We saw an example during Katrina where the region needed communications to recover but they needed transportation recovery to repair communications – the same with the power, the same with the water and it is still taking a long time to get systems restored. In general, we don't have plans for recovering from such large-scale failures.

We also don't have the ability to analyze large scale failure modes. The Commission developed some simple models which showed that cascading failures sometimes turn around, but sometimes keep growing yielding infrastructure service availabilities asymptotic to zero. Such situations, if true, would make recovery very difficult. I lay down this challenge to you: we need to develop modeling capabilities capable of analyzing complex, interconnected infrastructure failure and recovery, including failures that occur simultaneously throughout the infrastructure. If you have good ideas, I know people who would like to talk with you.

The Commission determined that large scale infrastructure failure from an EMP attack is a problem that couldn't be solved, but would need to be managed. On the one hand we don't want to give our adversaries a free shot at us. On the other hand it would take a major part of our gross domestic product to make sure we're absolutely invulnerable to the effect. See Figure 9

The same is true for hurricanes. A strategy is presented in the chart above. The Commission recommended that we what we can, starting at the lowest cost end of the spectrum and move forward. Some of the less expensive things to do are to try to prevent attacks, prepare to recognize them, protect the most vulnerable and critical portions of the infrastructure including SCADAs, and then plan for recovery. Cost-effective EMP protection methods are available for critical systems as indicated in the chart below.

See Figure 10

A non-trivial problem is recognizing an EMP attack if it has occurred. The status of the infrastructure is reported back through communications lines that are, themselves, vulnerable. The power blackout of 2003 had that problem – operators kept saying I don't know what we've got out there – which transmission lines are up? We need to protect the system status-monitoring systems so we know what's happened and how to respond and recover. It will be important to red team this. We shouldn't assume the people responsible are going to do it, or even know how to do it. See Figure 11

Government can't do it all. There should be sharing to develop and implement solutions between industry and government. The Commission believes the Homeland Security Council and the Department of Homeland Security should have major responsibility with identifiable people having authority to address the wide-scale threat issue (see the following chart). And I would recommend that they address it in terms of wide-scale phenomena in general, not just EMP.

See Figure 12

In conclusion, EMP is one of a very few potentially catastrophic wide-scale threats to the United States. By taking action, the EMP threat can be reduced to manageable levels over time. A national strategy to address the EMP threat should balance prevention, preparation, protection, and recovery.

If you would like to read our executive summary, here is the website: http://empcreport.ida.org

Question from audience: What kind of effects would EMP have on our satellites?

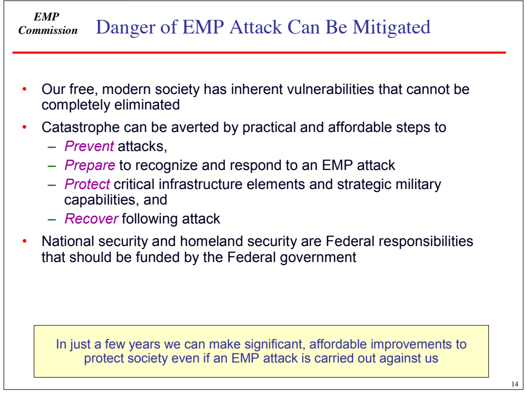
Response from Dr. Graham: Nuclear weapon effects on satellites stem mostly from their X-ray output, not EMP. X-ray output will affect satellites 1000's of kilometers from a high altitude burst. Low earth orbit satellites are highly susceptible to failure from exposure to X-rays, and trapped electrons.

Panel One – Prevention

Introductory Comments: Mr. Dutch Thomas, MSA Inc. (Moderator)

Mr. Thomas provided a special welcome to international students attending the symposium from the National Defense University. Commenting on Dr. Graham's presentation, Mr. Thomas indicated that some Russian military radio vans still incorporate vacuum tubes, a technology from the 1950s, in their design. There is good reason to believe that this older technology is still used because it is more resistant to nuclear EMP effects than are transistors and integrated circuits. In discussing infrastructure assurance, we need to consider a full range of solutions which might involve using older technologies. Not all preparations need to be complex. Sometimes the most

Figure 9



EMP Commission

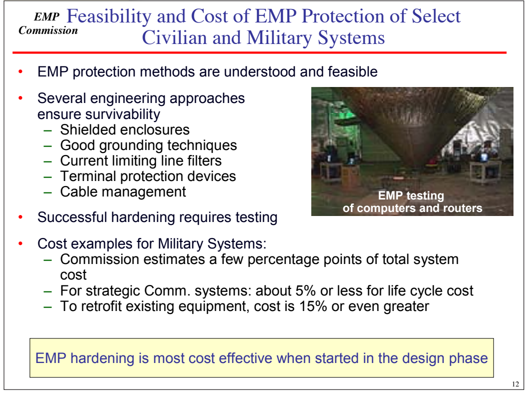
Danger of EMP Attack Can Be Mitigated

- Our free, modern society has inherent vulnerabilities that cannot be completely eliminated
- Catastrophe can be averted by practical and affordable steps to
  - *Prevent* attacks,
  - *Prepare* to recognize and respond to an EMP attack
  - *Protect* critical infrastructure elements and strategic military capabilities, and
  - *Recover* following attack
- National security and homeland security are Federal responsibilities that should be funded by the Federal government

In just a few years we can make significant, affordable improvements to protect society even if an EMP attack is carried out against us

14

Figure 10



EMP Commission

Feasibility and Cost of EMP Protection of Select Civilian and Military Systems

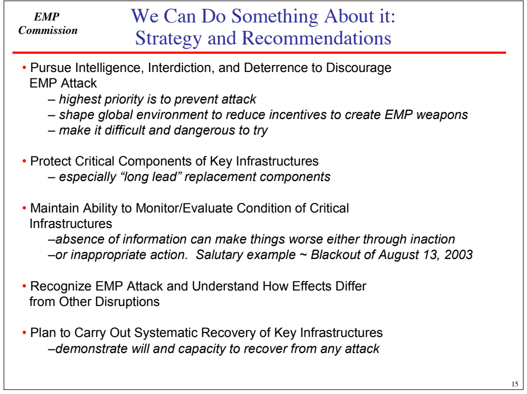
- EMP protection methods are understood and feasible
- Several engineering approaches ensure survivability
  - Shielded enclosures
  - Good grounding techniques
  - Current limiting line filters
  - Terminal protection devices
  - Cable management
- Successful hardening requires testing
- Cost examples for Military Systems:
  - Commission estimates a few percentage points of total system cost
  - For strategic Comm. systems: about 5% or less for life cycle cost
  - To retrofit existing equipment, cost is 15% or even greater

EMP testing of computers and routers

EMP hardening is most cost effective when started in the design phase

12

Figure 11



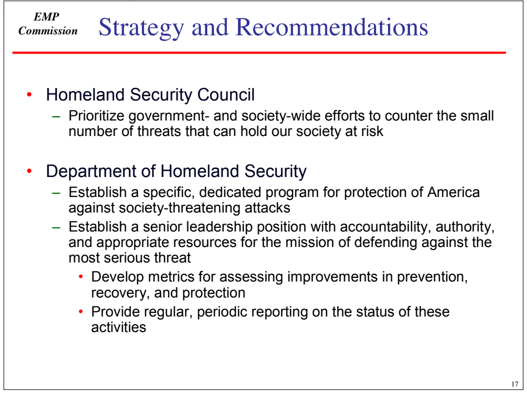
EMP Commission

We Can Do Something About it: Strategy and Recommendations

- Pursue Intelligence, Interdiction, and Deterrence to Discourage EMP Attack
  - *highest priority is to prevent attack*
  - *shape global environment to reduce incentives to create EMP weapons*
  - *make it difficult and dangerous to try*
- Protect Critical Components of Key Infrastructures
  - *especially "long lead" replacement components*
- Maintain Ability to Monitor/Evaluate Condition of Critical Infrastructures
  - *absence of information can make things worse either through inaction*
  - *or inappropriate action. Salutary example ~ Blackout of August 13, 2003*
- Recognize EMP Attack and Understand How Effects Differ from Other Disruptions
- Plan to Carry Out Systematic Recovery of Key Infrastructures
  - *demonstrate will and capacity to recover from any attack*

15

Figure 12



EMP Commission

Strategy and Recommendations

- Homeland Security Council
  - Prioritize government- and society-wide efforts to counter the small number of threats that can hold our society at risk
- Department of Homeland Security
  - Establish a specific, dedicated program for protection of America against society-threatening attacks
  - Establish a senior leadership position with accountability, authority, and appropriate resources for the mission of defending against the most serious threat
    - Develop metrics for assessing improvements in prevention, recovery, and protection
    - Provide regular, periodic reporting on the status of these activities

17

effective solutions might involve simpler techniques to be found in history and in the life style that preceded our modern complex technology-driven culture.

Remarks of Panelist Taz Daughtrey, Department of Computer Science, James Madison University.

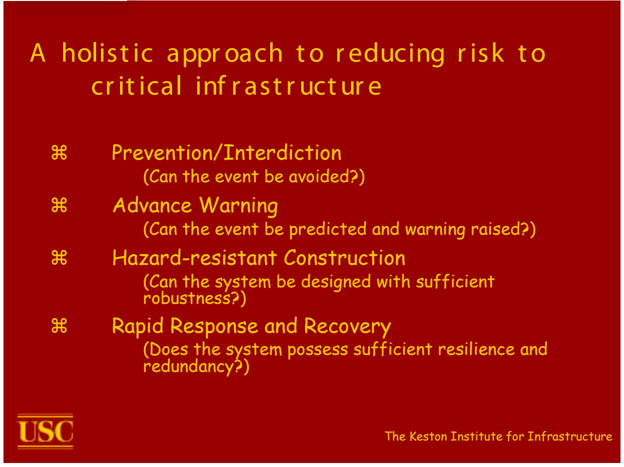
An important part of the homeland security endeavor is assessing risk associated with threats and hazards. Mr. Daughtrey set the stage by defining risk and considering methods for analyzing risk, focusing on cyber security as a key component of prevention.

Put simply, today's risk is a problem that we don't want to have happen tomorrow. Yesterday's problems are part of today's risks, but we try to avoid today's risks as tomorrow's problems. As we look at managing risk and look at situations that produce conditions we would find unacceptable, we classically divide potential solutions into two categories: risk avoidance and risk mitigation. It is appropriate in this panel, as we explore prevention, to talk about risk avoidance. Later panels on protection and response will treat methods of minimizing the consequences of an adverse event. Prevention involves minimizing the probability that the event will occur in the first place. There must be a balance among the approaches. We can't achieve zero probability that bad things will happen – such guarantees are cost prohibitive. There will always be a certain amount of risk exposure that we have to bear. But on the other hand, we can't shift our attention entirely to response and recovery after the event.

Cyber security is a major object of prevention measures since cyber systems are used in the operation of most infrastructure. All of us are aware how much we depend on computers and software. It has become one of the great curses of society. A few years ago the number one excuse for inaction was, "The check is in the mail." That has now been surpassed by the number one excuse, "I'm sorry, but my computer is down." When we try to make reservations, leave messages, or make financial transactions, if the computer is down, nine times out of ten there is no fall-back position. This is illustrated by a cartoon in which an administrative assistant in an office answers the phone by saying, "Our computers are down. I'm having to do everything manually now." And the assistant has a deck of cards in hand, playing solitaire. Here's a rare example where there is a backup system for a computer program.

One of the greatest concerns across the academic and industrial spheres, is to reduce the vulnerabilities that are all too typical in software. Recognizing the extent of our dependence and the ways we would suffer from the consequences of both inadvertent and the increasing number of deliberate attempts to bring down computer services, from a prevention point of view, we need to minimize the vulnerabilities. In the education and research arenas, we must make sure that the next generation of software developers is aware of the very widely known and easily

Figure 13



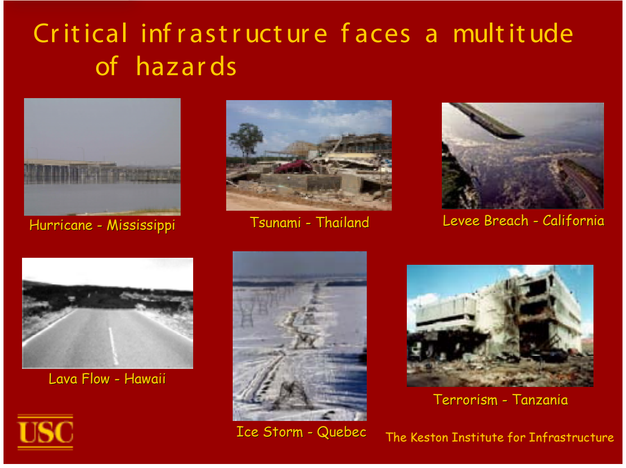
A holistic approach to reducing risk to critical infrastructure

- ⌘ Prevention/Interdiction
  (Can the event be avoided?)
- ⌘ Advance Warning
  (Can the event be predicted and warning raised?)
- ⌘ Hazard-resistant Construction
  (Can the system be designed with sufficient robustness?)
- ⌘ Rapid Response and Recovery
  (Does the system possess sufficient resilience and redundancy?)

USC

The Keston Institute for Infrastructure

Figure 14

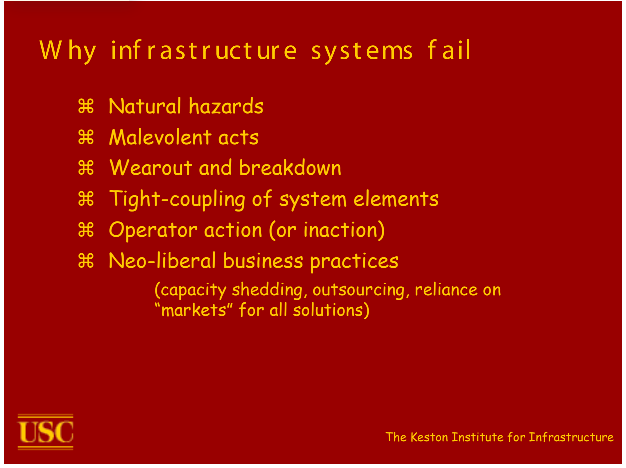


Critical infrastructure faces a multitude of hazards avoidable vulnerabilities that people have allowed to be built into or to creep into our systems. We have a tremendous backlog of software and systems that easily exploitable vulnerabilities. While it is of critical importance that educators convince folks just to be more careful, we are developing a rigorous prevention methodology we call secure software engineering. We now don't just focus on software/system functionality, but also address the security and dependability of systems. The "gee whiz" of getting the software to work shouldn't overwhelm our concern about removing vulnerabilities.

On a broader arena, because the users of software are probably the biggest vulnerability, we need to educate the whole user community drawing on social engineering techniques. We are addressing this concern in K-12 and the general public by developing guidance on safe computing practices addressing the ways that people configure and use their computers to receive, send and store data. These are all part of the risk avoidance – of prevention.

In the cyber area there is a lot of low-hanging fruit. In terms of what we build into the systems and how people use systems, the bad news is that it's unfortunate there are still a lot of vulnerabilities. The good news is they're fairly easy to correct. If we can convince software developers to avoid buffer overflows and a dirty list of the top ten problems this would eliminate 90 percent of the vulnerabilities out there. If we convince the general citizenry to be more careful and attentive to how they're using computerized systems, then we could start to tackle the remaining, really difficult problems. I believe that we can greatly reduce our risk exposure through rather straightforward activities.

Figure 15



Why infrastructure systems fail

- Natural hazards
- Malevolent acts
- Wearout and breakdown
- Tight-coupling of system elements
- Operator action (or inaction)
- Neo-liberal business practices
  (capacity shedding, outsourcing, reliance on "markets" for all solutions)

USC

The Keston Institute for Infrastructure

Remarks of Panelist Richard Little, Director of Keston Institute of Infrastructure, University of Southern California.

We hear a lot about malevolent threats. Certainly a lot of people will address these at today's symposium. But one of the major implications of our Katrina experience last year is that homeland security involves more than dealing with terrorism and malevolent threats. We need to achieve a balance in attention to natural hazards and malevolent threats.

First off, how do we really think about reducing risk? The chart below lists four risk reduction methods. First we ask the question, how can the event be avoided? See Figure 13

We hope we can prevent attacks. But there are certain situations, like Katrina, and earthquakes in which the best thing we can do is give some warning and then get out of the way. Later panels will address protection which gets into system design and building systems that are robust enough to resist a whole range of insults. Finally, when the first three strategies fail, we get the systems back up and running due to their resiliency. See Figure 14

If we look at the kind of hazards that infrastructures face, there are natural hazards and malicious hazards. Looking at the pictures in the chart above, it appears the consequences of natural and malicious insults are similar. We can approach risk management to both classes of hazards in a similar way.

A useful approach is to look at why infrastructures fail. The following chart lists five basic reasons: See Figure 15

We tend to underinvest in the less glamorous causes and, as a result, are allowing our infrastructures to seriously deteriorate. Tight coupling is inherent in electronic controls. If we didn't depend on all those electronic gadgets, EMP wouldn't be such a serious threat. A lot of events precipitate and cascade because the people that are part of the system either don't know what to do – or what they know to do turns out to be wrong.

Neo-liberal business practices that look to the market to provide all solutions, have led to such things as very lean organizations, capacity shedding, just-in-time deliveries, and outsourcing which seriously increase system vulnerability. Here is an example from California on how this might occur. See Figure 16

There is a rather fragile system of flood levees in California whose maintenance has been deferred due to budget shortfalls. Even a moderate earthquake may lead to a breach which leads to flooding, possible loss of life, and damage in the billions of dollars. This is all known. It's a fairly simple system, but going back to the cause of the phenomenon, people fail to make this kind of connection.

As you deal with homeland security and various types of catastrophes, keep this chain of events in mind. And remember that you can get the same kinds of failures with different causes but basically the same outcome.

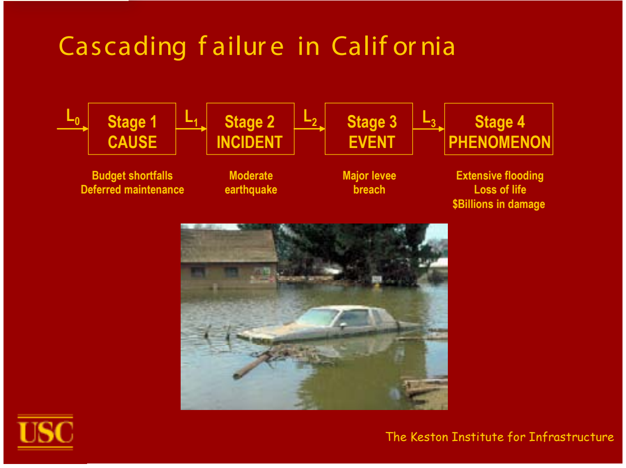
See Figure 17

The chart above shows four broken bridges with the same effect – inability to get from point A to point B. The causes were quite different, including an earthquake, deferred maintenance, flooding, and a ship collision. Another panelist, Taz Daughtrey began to talk about probabilities – it's really just a lot of conditional probabilities. If we can calculate the probability of a bridge collapse during an earthquake of a certain magnitude, we can develop a risk calculation formula in terms of dollar cost. We can also then figure the benefit of reducing the impact of cascading failures.

Be careful with terminology. Vulnerability is not the same as threat which is not the same as risk. Often they are used interchangeably. Vulnerabilities can exist in the absence of a threat. You may have noticed that the area around this building and the State Department and Federal Reserve has become a poster child for preventing intrusions of truck bombs into public buildings. We have just about every example of prevention and protection you can find. That's because buildings are vulnerable to truck bombs. But the actual threat is perhaps more difficult to determine. It is straightforward to reduce vulnerabilities – but not so for threats. We need to consider both, taking into account multiple threats. And vulnerabilities and threats must be congruent. See Figure 18

The Maginot Line really was impenetrable – so the Germans went around it. The lesson is that we need to

Figure 16



Cascading failure in California

L_0 → Stage 1 CAUSE → L_1 → Stage 2 INCIDENT → L_2 → Stage 3 EVENT → L_3 → Stage 4 PHENOMENON

Budget shortfalls
Deferred maintenance

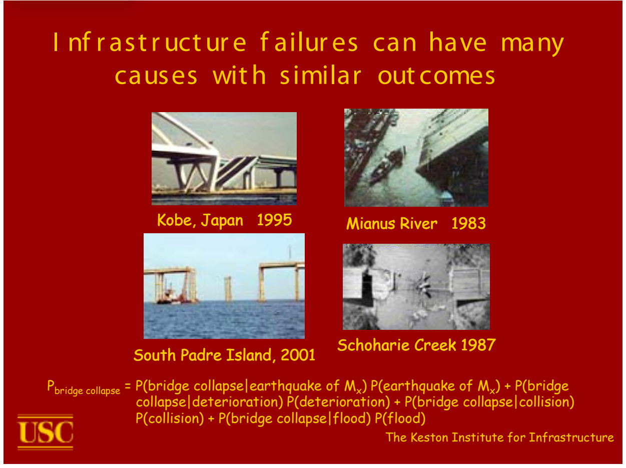
Moderate
earthquake

Major levee
breach

Extensive flooding
Loss of life
$Billions in damage

The Keston Institute for Infrastructure

Figure 17



Infrastructure failures can have many causes with similar outcomes

Kobe, Japan 1995

Mianus River 1983

South Padre Island, 2001

Schoharie Creek 1987

$P_{\text{bridge collapse}}$ = P(bridge collapse|earthquake of M_x) P(earthquake of M_x) + P(bridge collapse|deterioration) P(deterioration) + P(bridge collapse|collision) P(collision) + P(bridge collapse|flood) P(flood)

The Keston Institute for Infrastructure

make sure our countermeasures address all the threats. When we respond reactively we tend to implement excessive responses.

See Figure 19

Finally, we really need to think about infrastructure as a commons. It's really not just a market type thing, but it's something from which we all take and we all ought to give back. We need to protect and manage this commons so the benefits are sustained. This means we need to demand strategic investments to overcome the issues that I've talked about. We need to get this right.

See Figure 20

Don't assume we won't make the same mistakes as earlier societies. We can learn from the mistakes of history.

Remarks of Panelist J. Peter Pham, Director, Nelson Institute for International Studies, James Madison University.

There's an old adage that says, "a diplomat is an honest man sent to lie on behalf of his native country." What any country needs is diplomats with an ability to be forthright with the information they provide at home and convey abroad.

The hydrocarbon infrastructure is an example of a microcosm of problems that we have with prevention in the world in which we live today and the security environment in which we find ourselves. Many of my colleagues at JMU are working on overcoming problems associated with our current energy dependence, but until that blessed day arrives, our economy and that of the world is still relying on hydrocarbons. Any impact on the hydrocarbon sector directly affects our infrastructures and our ability to continue to carry out the tasks that we've set out for ourselves.

Critical infrastructure reliance on hydrocarbons starts with hydrocarbon production. And that is where we have a blind spot relative to prevention. To address this, I considered three concerns: definitions, monitoring, and ultimately, partnership.

If hydrocarbons are important to us, where do we get them? If you were to poll Americans in the street,

Figure 18

Failure prevention strategies must address multiple threats

The New York Times.
TITANIC SINKS FOUR HOURS AFTER HITTING ICEBERG; 866 RESCUED BY CARPATHIA, PROBABLY 1250 PERISH; ISMAY SAFE, MRS. ASTOR MAYBE, NOTED NAMES MISSING
THE MAGINOT LINE

USC

The Keston Institute for Infrastructure

Figure 19

Reactive responses to failure are often excessive

Police Concede Slain Suspect Not a Bomber
Security Efforts Turning the Capital Into an Armed Camp
Scaring Us Senseless
We aren't wired to respond rationally to terrorism.

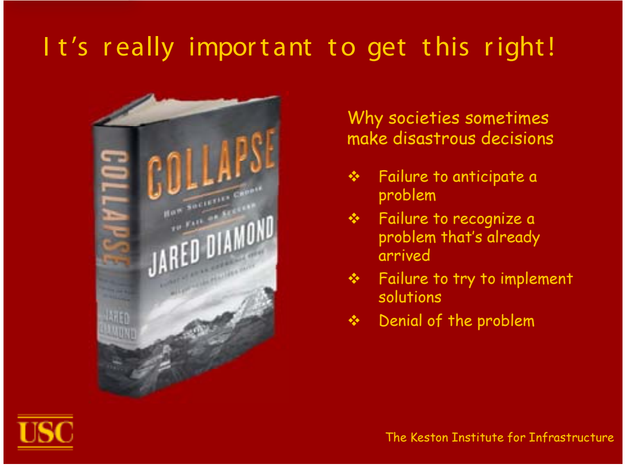
New York Times, 2/22/04

New York Times, 7/24/05

USC

The Keston Institute for Infrastructure

Figure 20



It's really important to get this right!

Why societies sometimes make disastrous decisions

- Failure to anticipate a problem
- Failure to recognize a problem that's already arrived
- Failure to try to implement solutions
- Denial of the problem

USC

The Keston Institute for Infrastructure

most of them would point to the Middle East. Most people don't realize that, slowly, our hydrocarbon needs are being met by other areas of the world. Currently 15 percent of the hydrocarbons we use in North America come from Sub-Saharan Africa. The National Intelligence Council estimates that within the decade, this fraction will rise to somewhere in the vicinity of 25-28%, far exceeding what we get from the greater Middle East. Yet we don't devote the resources to monitoring this source that we do to the greater Middle East.

With regard to "definition," how do we define threats and vulnerabilities relative to this particular supply area? Because of a question of definitions we don't define very many threats in this part of the world. The State Dept's annual report, for example, "Patterns of Global Terrorism," almost never lists events in Sub-Saharan Africa. The last time the State Department admitted there was terrorism in Sub-Saharan Africa, was in 2003 where they listed just 15 incidents – again because of technicalities related to definitions. Obviously, the terrorist problem is larger than what is being reported.

> *Most people don't realize that, slowly, our hydrocarbon needs are being met by other areas of the world. Currently 15% of the hydrocarbons we use in North America come from Sub-Saharan Africa.*

Second concern related to prevention through diplomacy is the difficulty of monitoring threats and vulnerabilities and ultimately, risks. From a diplomatic standpoint, the whole region is uncovered. Our largest source of hydrocarbons is Nigeria. Yet in the volatile northern part of Nigeria we have no consular presence and haven't had one for decades. The last time I was in Nigeria, about a year ago doing research, there was not one Foreign Service officer fluent in the major languages of northern Nigeria. Many developments are missed or unreported because religion is not monitored. Although religion doesn't cause terrorism, it is known that it can foment and inflame it.

The final diplomatic aspect of prevention is developing the right partnerships to monitor critical parts of the world to assistlocal US capabilities. This is something we need to do to get beyond the dead-end dialectic with respect to these blind spots. We need to get beyond models that may have worked for us in a certain time history. The world has changed and our interests have shifted but in many cases structures for incentives for career diplomatic officers, structures for analysis, and strategic vision are caught in a previous mindset. Our prevention capabilities are severely hampered by our previous models and ways of thinking.

Prevention Panel Summary

Dutch Thomas summarized the panel proceedings. Presentations addressed physical infrastructure, cyber infrastructure, new thinking, and diplomatic solutions. He asserted that it is not possible to prevent all attacks, rather we need to plan to mitigate their effects. Those best able to do this are at the local level. This is somewhat the antithesis of the Homeland Security Act. We need community-based national preparedness. Mr. Thomas then opened the floor to questions.

Question from audience: Does analyst training include chess?

Response from David Moore: Although chess is not part of the formal training, many of our trainees are chess-players. At the National Security Agency, the most successful analysts like puzzles, games – activities with rules and strategies, and moves.

Question from audience: There is a study by Richard Hackman of Harvard on what makes intelligence teams more or less effective. The gist of his study of 27 intelligence agencies was that well-formed, well-managed teams were much more productive than groups of brilliant thinkers. In your training program, how do you make a distinction between developing individuals' capabilities vs developing teams of people working together to think and produce more effectively.

Response from David Moore: We are looking at the benefits of a cooperative and competitive work environment in enhancing both analyst reasoning and function. There are studies that show the importance of both sides of the coin – brilliant individual thinking vs. team thinking, collaboration vs. competition. The key is, as you mentioned, effective management of the team itself that allows for the innovation to occur. Different points of view must be present. Robert Callum's study in the International Journal of Intelligence and Counterintelligence looks at this issue in great depth. He argues that cross-cultural teams bring to the table different mindsets and biases, that when everything works well, team members offset each other to get to the best solution. On the negative side, groupthink occurs within teams. It is not a simple issue of throwing good people and good management in a room together and throwing a problem at them. It's akin to throwing young princesses into a room filled with straw and asking them to weave gold. In either case, elves don't seem to pop through the floor to help them out.

Response from Rich Little: A lot of the physical failures that I addressed and many others that I've looked at could have been predicted. It's not so much a question of not knowing what bad things are going to happen, but an organizational culture that was unreceptive to the message. I would like to caution that you can have the best analysts in the world but if they're operating in a culture that is not receptive to things that run counter to what they want to hear, you're not going to get good results. Look at both the Challenger and the Columbia disasters; look at the Northeast Power blackout and a couple of the bridges I talked about. In these cases, there was known predictive information, there were reactions based on civil system rules, and most people failed to act because of organizational-cultural issues. This is an enormous problem.

Question from audience: What can be done to correct the stove-pipe approach to our critical infrastructure which is a system of systems? For example, the banking infrastructure has a recovery time objective of four hours. It is not apparent that they are coordinating with the electrical and telecommunications infrastructure. A problem exists with coordinating the interdependencies among the critical infrastructure sectors. There appears to be a lack of will to coordinate the hard problems among them. It's a problem caused by distributed supervisory control.

Response from Taz Daughtrey: When people say we are OK within our own system, have they taken into account the ramifications of their dependence on other systems? Unfortunately, it takes a catastrophe for people to realize this.

Response from Dutch Thomas: It is a human interface problem. During routine operations, infrastructure service providers have a sense of ownership and possessiveness of their systems. The interconnectivity and interdependence is often not part of the routine day. The situation also occurs between volunteer organizations that have an emergency response mission. Human nature mitigates against sharing information on one's own system that might give away vulnerabilities. Interaction between system operators is key. There is also a vocabulary problem due to the multi-tiered nature of the problem spanning different system communities, often over large regions.

Response from David Moore: This is a very hard problem. It gets right to the heart of a new discipline called Complexity Science. We're dealing with complex adaptive systems here. They exhibit emergent behavior, they learn, they adapt and there is research within the field of complexity that can inform and assist in developing solutions.

Response from Richard Little: I think the critical point that you raise is that many of these sectors have in fact solved their own problems reasonably well. The banking system is well-positioned to deal with some of these issues. What hasn't happened is widespread transference of vulnerability and response information from some of the sectors that have done better. The problem is exacerbated by what I call "neoliberal business practices" in which we rely totally on the market to work out its own issues. The fact of matter is that a marketing solution for the banking industry may not be the best solution for the nation as a whole. My opinion is that, until the government at the national level steps up to say that there are higher level objectives other than market forces across sectors, we're not going to get help. And ultimately that's what is going to happen, because the individual sectors will maximize their own business utility functions for themselves and that's not a way to manage the commons.

This is an area that probably doesn't need better research – it needs better implementation.

Response from Peter Pham: The point you raise is a very important one. I think part of the issue is ultimately a social question. We can use some of the work that has already been done using social interaction and complex system theory to try to mitigate the problems. Human nature is the biggest hurdle. Also, the U.S. can break down barriers at state and national level – but there remains a problem that many of the systems in question are transnational.

Question from audience: In military systems there is a lot of pressure for total system integration. The Navy builds ships that are totally integrated – everything is initially designed to play together. When we go out to do operational testing on systems, the operational test measure of system availability gets tested. When we test a system, we ask an operator to perform a function and many times they can't. When looking for why, the answer is often the lack of input. The system's lights are on, it's working. But in order to have function, the system depends on someone else's system. It's fine to want a 0.95 availability function, but if the system depends on other systems that also have a 0.95 availability, my real functional availability gets pretty low. People often ignore this. With complex systems, the key to integrating systems is understanding fault tree and critical path analysis. It is not possible to randomly take shots at individual systems and expect to fix them all. Is there any good work being done using probability theory including Bayesian approaches to systemically lay out critical paths?

Response from Dave Moore: Yes. If we're looking at the end of the critical path, there are very few options. There are a lot of options upstream. Classic warning is an example. It is important to have information on catastrophic events as early as possible. The action lag time of affected users that have received a warning gets shorter and shorter as the event approaches. But they need to recognize that they have a larger set of options early on in a situation.

Response from Taz Daughtrey: We also need to recognize economic benefits of early action. It's much better to work upstream rather than downstream on the critical path. In the development of systems, and particularly software-based systems, there's some pretty good empirical data that the growth in the cost of finding and fixing defects is almost exponential across the development life cycle. So obviously, the sooner you recognize a problem, the wider the range of available options. We should avoid trying to solve the problem by using patches once failures start occurring.

Question from the audience: This panel addresses 'prevention.' Some attacks can't be prevented. I am concerned about a lack of communication to the lay public. The public is not getting the information they need to prepare and respond. Do you have any suggestions on improving the communications to the lay public and educating them in this area?

Response from Rich Little: There has been an enormous amount of work done in risk communication, particularly risk communication related to natural hazards. It's interesting that one of the things the scientific community always told the Congress years ago was just give us more money and we'll get better at predicting things. Actually, in the case of hurricanes path prediction, they're getting really good. And the warning message to the affected coastal areas before Katrina was very accurate – leave or you will die. But the human response to warnings gets into how people believe and process the warning information and act upon it. It's interesting that the evacuation of Houston was so much more extensive than that of New Orleans. People who live in New Orleans have a mind set. Based on prior experience, many people figured they could live through any hurricane, not realizing that Katrina's consequences would be quite a bit more severe. It takes a long time for mindsets to wear down. There has been a lot of criticism of the DHS color scale warning system. People don't know how to respond to this. So it's more than just getting the message out to people – we need to figure out how to reduce action lag time. Unfortunately, from a hazard standpoint and certain types of attacks that could actually happen, people are just as likely to call their brother-in-law who works in a certain agency to find out what to do. People are skeptical of public pronouncements. It's based on "who do you trust – who do you believe?" It's not a perfect system. This is an area that probably doesn't need better research – it needs better implementation.

Featured Speaker

Remarks by Daniel W. Caprio, Jr., Senior Fellow and Executive Vice President, The Progress and Freedom Foundation

The internet has revolutionized communication. We stand on the edge of an era that will introduce unimagined network devices and objects with an ability to combine and use data from multiple, diverse sources in informative and compelling ways for the benefit of our citizens, societies, and countries. We see the cost of storage, processing and communications are dropping. Devices are becoming smaller and cheaper, more capable, communicative and interconnected, and uniquely identified with new tools emerging for aggregating, sharing, searching and distributing data.

The research from VDC Corp. estimates that the market for RFID reached nearly $1.8 billion in 2004 and will reach $5.9 billion in 2008.

Dr. Caprio views RFID technology as the sweet spot in IT innovation. It is a technology that is rapidly evolving and promises huge benefits with respect to economic growth, and competitiveness. The technology is of great interest to policy makers because it offers sweeping improvements in privacy, security, standards, interoperability and spectrum. RFID promises to lower cost for managing inventory, reducing error rates, inhibiting counterfeiting, improving product visibility, improving drug safety, allowing elderly Americans to age in place. There are also many applications in homeland security.

Here are some of the potential economic benefits from some forecasting firms. The research from VDC Corp. estimates that the market for RFID reached nearly $1.8 billion in 2004 and will reach $5.9 billion in 2008. The Wireless Data Research Group estimates the market will grow from $1 billion in 2003 to $3 billion by 2007. The Gartner Group forecasts worldwide RFID spending will surpass $3 billion by the year 2010.

So what is RFID? RFID is one of several automatic identification sensor-based technologies consisting of three key elements: a tag, a reader, and a system of data collections and distribution that allows for the management system to identify and scan information with increased speed and accuracy. Readers can sense tags from distances, and read ranges vary depending on the type of tag. Some common applications of RFID that we are already becoming familiar with today include: E-Z Pass, access cards to facilities and subway system, the mobile speed pass, anti-theft keys for your automobile, and marathon competition timing chips.

RFID technology is being introduced increasingly in the supply chain beginning at the factory. At point one raw materials can be tagged so that a manufacturing company knows precisely how much is used in the manufacturing process. RFID offers the ability to monitor plant conditions; where sensors can be built into the tags to monitor humidity and temperature. In the warehouse, the scanners can be used on loading docks to track incoming pallets and items. As goods are transported out of the warehouse, leaving the gate, the contents of a container can be verified and scanned. As products arrive at a store, they can be scanned on the backend. This is a major benefit of RFID as opposed to barcode technology. Products are visible to RFID sensors without requiring direct line of sight. RFID inventory tracking ends at the checkout counter.

RFID technology can be tailored to the application. On the road, passive RFID tags can be used to seal the door. Active tags can be used as intrusion sensors providing organic communications back to a central tracking computer. At port locations tags can be used for identity as well as sensing and intrusion detection. Pharmaceutical product tracking RFIDs can be used to prevent counterfeiting. Pfizer and Purdue-Pharma today are beginning pilots and putting RFID tags on pill bottles and that reduces unauthorized access at the wholesale and pharmacy level. Other health care industry examples includes use of RFID technology by Texas Instruments to track blood; Intel's use of RFID on surgical devices. Food safety is another important application where RFIDs are outfitted with temperature sensors to ensure that products have maintained chill compliance throughout the supply chain. RFID can be used and is being used to identify products by batch code when recalls are necessary. Kroger, for instance, is using RFID to track food from the point of origin.

In the transportation safety enterprise, Delta Airlines is using RFID technologies to monitor the performance of aircraft engines in terms of their maintenance supply and regimen. Delta is already seeing an immediate return with maintenance costs being reduced by half. Very recently, Boeing has announced that they are going to be using RFID in the new 787 Dreamliner. Relative to road vehicle safety, we're beginning to see RFID being used to monitor tire pressure. This application also reduces wear on tires and fuel consumption.

Internal business applications are manifold. Hewlett Packard is tagging cartons for PCs, printers, and ink cartridges. HP projects a number of internal benefits including increased speed and efficiency of manufacturing and distribution, improvements in transfer and increased product offerings including the manufacture of computers to individual specifications.

Retail experience is being driven by Wal-Mart and the Department of Defense. Wal-Mart began requiring their top 100 suppliers to tag their goods beginning last year. Wal-Mart is already beginning to see benefits. Both Wal-Mart and Target have been able to improve on-shelf availability of their products. A study by the University of Arkansas indicated that Wal-Mart reduced their out-of-stock items by 16 percent, very significant in the retail business. RFID has also reduced Wal-Mart's costs associated with inventory handling, warehouse facilities, and waste.

The Department of Defense is following Wal-Mart's example by using RFID within its logistics supply chain. DoD is expected to spend roughly $500 million over the next six year period on RFID. The implementation of RFID in the Marine supply chain has cut inventory value in the chain from $127 million to $70 million. Average delivery times have dropped from 28 days to 16 days. Supply backlogs have fallen from 92,000 shipments to 11,000. DoD, using active RFID technology, now knows where products are in the supply chain reducing the volume of warehouse supply backups.

As the EZ-Pass example illustrates, RFID use need not implicate personal privacy. What we need at this point is a comprehensive public/private partnership to create voluntary market oriented self-regulatory guidelines that respect and protect the need for privacy and security. The guidelines should give consumers tools and choices they need to protect themselves, while sustaining innovation. As RFID drives innovation, it is important that system architectures be designed with built-in privacy and security.

For RFID technology to really begin to take hold and gain broad acceptance, we need accurate information about the technology, the opportunities, the challenges, and a continuing instructive dialogue. Recently, a number of companies and some civil society groups announced the formulation of best practices for RFID technology use. Cisco, Eli Lilly, IBM, Intel, Microsoft, Proctor and Gamble, Verisign, VISA, Center for Democracy and Technology, and the National Consumers league were involved. The group developed an agreement for how consumers should be notified about RFID collection of consumer information. The agreement included the need for clear and conspicuous notice when information is collected through an RFID system, notice and choice before the conclusion of a transaction, access to the information if it is maintained on the tag, and reasonable and appropriate security to secure those RFID tags.

With so many potential applications, RFID is in the sweet spot of technology policy development.

RFID represents one of a set of technologies that are transforming business methods. The technology essentially enables an "Internet of Things." RFID has the potential to be able to identify machines, identify objects, understand their status, and communicate and take action if necessary to create "real time awareness." It fosters the convergence of communications, computing, and interactivity means that are available in most locations through wireless, sensors, and network computing systems.

Plans for sensor networks are proliferating, bridging the physical and virtual world to include smart buildings, transport, cars, and monitoring for the elderly. We're moving into the next RFID adoption phase within the next two to three years. "Aging-in-place" is one of the next big applications as are environmental scanning, detection of bioterrorism, and making those supply chains transparent.

Relative to preparedness for disaster, consider the "Internet of Things" and the world ten years from now. We've just come through with Katrina and a Tsunami. RFID offers the potential to monitor the environment, to monitor structural integrity, the presence of water, the presence of toxic substances, to be able to monitor people, to be able to have first responders tracked via improved communication devices, to be able to locate victims via building monitors, monitoring goods, inventory and distribution of emergency supplies, automatic reordering, and location of high value medical and rescue equipment. With so many potential applications, RFID is in the sweet spot of technology policy development. As the technology is becoming more widespread, we now need to get the policy choices right with respect to privacy, security, inoperability, standards and spectrum.

The Department of Commerce offers several resources pertaining to RFID technology. The Department organized a workshop in April 2005 that issued a report on RFID technology available at www.technology.gov/reports.htm. There is an RFID Intragovernmental Council which is a group representing all of the Executive Branch agencies and some of the independent agencies. The Office of Management and Budget is currently addressing policy issues related to RFID. Federal applications will lead the way in developing privacy and security issues particularly with respect to DHS, the U.S. Visa Program, and the State Department's electronic passport program. These will be very important efforts in developing public adoption and trust. One final resource is the Federal Trade Commission's trade workshop of June of 2004 which issued a comprehensive report in May of 2005 which is posted at http://www.ftc.gov.

Question from the audience: What's the biggest impediment to realizing the "Internet of Things?"

Response from Mr. Caprio: That is a good question because business process reform is a big part of RFID. The issues going forward will be dominated by the policy questions. We're seeing broad technology adoption and pilot programs in a number of industries. A year or so ago, the prevalent thought was that RFID applications would occur primarily in retail item tagging. That's been a little slower to grow because of the system cost. Widespread adoption will occur as the price of RFID chips and readers comes down. Price is affected by standard development, interoperability, some of the spectrum issues, and some global issues in China. China is very important to this because, for example, 65-70% of Wal-Mart's are manufactured in China. While I was in the government we were working very hard with the Chinese on developing a standard that will allow for interoperability. We don't necessarily need a harmonized spectrum - but we do need the ability to interoperate.

Panel Two – Protection

Introductory Comments: Patrick Bridge, Coordinator of Emergency Preparedness & Response Program Training for the Virginia Department of Health (Moderator)

Mr. Bridge thanked James Madison University and IIIA for inviting him to speak and for their support of the Virginia Department of Health (VDH) education efforts which he introduced during his presentation.

At VDH, protection and prevention really overlap in their activities. There are enormous challenges related to protection. We have more people and things to protect than we've ever had and we have more threats from which we need protection than ever. A lot of what we deal with in the Health Dept is looking at protection against bioterrorism. Terrorist threats range from explosives, chemical/biological attacks to radiological nuclear threats. We are also concerned about cyber attacks and identity theft. Obviously, we've had experience with hurricanes right here in Virginia so we know that is a threat. Bird flu prevention and protection are currently major efforts within VDH.

The program at VDH takes an all-hazards approach, addressing everything from bioterrorism to natural disasters including likely events that pose potential public health emergencies. Much of what we do is planning and partnering.

All disasters are local disasters.

The Federal government cannot protect everyone from everything. Right now, thanks to the foresight of Governor Warner and the continued support of Governor Kaine, all Virginia, by the end of this year, will have taken a terrorism and security awareness orientation class. One of the sections of this class deals with potential targets. When you think about Virginia, we have two main north-south interstates – I-81 and I-95. We have nuclear plants, tunnels, and bridges. We have bridges that are also tunnels. We have the National Capital Region, military bases, and one of the nation's largest ports, Hampton Roads. So we have many things to think about protecting in the Commonwealth.

We need to shift focus away from the idea that the federal government will be there for everything and look to local governments, business leaders and private citizens to invest in protection of infrastructure, and take more personal responsibility for family preparedness. In Virginia, a big part of this shift in focus is education. Each health district is doing flu planning, pandemic flu planning, and holding summits within communities. Preparedness must be viewed as a local issue. We are emphasizing preemptive education and a better informed public. We know that education will reduce panic and save lives.

In planning for health problems like small pox and the flu we designate what are called PODS or "points of dispensing." These are a very important part of our responsibility for public health in a potential crisis. "Epi-surveillance" is tracking the spread of infectious disease. This is another major responsibility within VDH.

Cooperation between the Department of Health and JMU's Institute for Infrastructure and Information Assurance (IIIA) has occurred related to planning for our dispensing sites. We are responsible for managing the strategic national stockpile, which consists of life-saving medications and supplies that the State can request from CDC. The system enables provisions to arrive at designated PODs within 12 hours of a request. The Department of Health will set up dispensing sites throughout the State if large numbers of people need to receive life-saving medication. Recognizing the need for creating awareness and trust within the communities, including minority populations, we enlisted the help of JMU to create a public health preparedness guide in both English and Spanish.

We regularly test our capabilities through exercises and drills. Since 2001, each health district organizes these every year. In October 2005, Virginia led a five-state exercise with surrounding states to the southwest, Kentucky, West Virginia, Tennessee, North Carolina and Virginia. It was a four-day exercise. The exercise addressed multiple threats. In October 2006 we are going to conduct another statewide exercise and that will be centered around our efforts for flu readiness. In these exercises we include as many first responder partners as possible. We usually get very good participation. In November 2004 we did an exercise in the Harrisonburg-Rockingham area. Part of that was to test our communications capability. We followed standard procedures. We realized after that drill that we have a tremendous Hispanic population in that region. We realized that none of the methods we used would have reached this population. To redress this problem, I enlisted the help of James Madison University and the IIIA. They were developing a preparedness guide. We were able to start with this and develop a corresponding Hispanic guide. We brought in Hispanic media and the Virginia Hispanic Chamber of Commerce to help with the planning. We looked at other nontraditional distribution for the guide. This will lay the groundwork for emergency communication to this community.

The key message in the JMU guide is the importance of personal family preparedness plans. The guide includes checklists. Most public preparedness guides are geared towards natural disasters. This is the first resource of its type to include the public health message as well. This is very important because viruses don't discriminate according to immigration status. We need to be able to reach and treat everyone affected.

This has been an excellent experience and example of public health, private business and academia working together. Each one of our partners brought a necessary and unique capability to the table which allowed us to develop and disseminate this guide. As with every program, a major challenge we face is funding. However, we believe that one of the most cost-effective approaches is preemptive education to help save lives down the road.

> *We are emphasizing preemptive education and a better informed public.*

Hurricane Katrina demonstrated that the federal government alone cannot handle a large scale emergency response. Likewise, a flu pandemic will require active engagement at the State and local levels. Localities will have the major role in response. States, localities, private businesses and the public must take measures to be prepared. One of the biggest challenges is that the public tends to have some very unrealistic expectations about the government assistance capabilities with respect to protection and prevention. During Hurricane Isabel, Virginians were fairly tolerant with no electricity for three days or four days. After this, all the good will was gone. The public outcry was, "Why isn't somebody doing something?"

The hurricane left a 200 mile swath where there was not an electric line or power pole standing. Power crews from 25 states were working very hard to restore the system. But people's tolerance was really very low. The same potential exists with regard to the availability of flu vaccine, were it necessary.

To sum up, every emergency is a local emergency and local protection and preparedness planning are key to a successful recovery.

Remarks of Panelist George Baker, Associate Director for Infrastructure Research, Institute for Infrastructure and Information Assurance

Many of my remarks will reinforce what you've heard from Patrick Bridge. Most of my professional experience has been here in Washington, at what once was the Defense Nuclear Agency, now part of the Defense Threat Reduction Agency. I am now an academic and in the "idea business. Six years ago, I moved from the Washington area to Harrisonburg, Virginia, and am now teaching at James Madison University. In Washington, I had a very top down perspective on the homeland security problem. From my vantage in Harrisonburg, I'm getting the opposite, bottom-up viewpoint. I can attest that the DHS message is not getting down to the local businesses and citizens in smaller municipalities such as Harrisonburg. A local public works official's remark is a propos: "The Homeland will be secure when our hometowns are secure."

We, as citizens, are really the front lines.

This is the "Protection Panel" and I want to emphasize the importance of the protection part of the equation. It is better to build a guard rail along a dangerous curve at the top of a mountain than to maintain a fleet of ambulances at the bottom. Much of the devastation of New Orleans that was attributed to the hurricane winds had nothing at all to do with wind damage. Most property loss was due to water damage that resulted from the failure of the flood <u>protection</u> afforded by the levies. In the wake of Katrina, it seems that there has been a shift in national emphasis to emergency response and recovery. As we seek how best to invest scarce resources, we need to determine how to balance protection and response measures.

DHS's National Infrastructure Protection Plan outlines a top-down strategy for protection of critical infrastructure. At the top are the responsible federal agencies. At the intermediary level, the plan includes a system of coordinating councils for each sector. These coordinating councils, as explained in the guide, are self-organized, self-run and self-operated by the individual sectors. Thus, the plan is not very prescriptive when it comes down to the grass-roots, down to the local level. The plan will succeed only to the extent that the local level infrastructure owners and operators become engaged.

We've all heard the statistic that 85 percent of the infrastructure is privately owned. We also need to remember that the other 15 percent, most of that government infrastructure, is owned and operated at the local and state levels. In our quest for infrastructure protection, it is clear that we will need to rely on the participation and judgment of local people – of the people on the ground – to the greatest extent possible. We need to push the planning down to the lowest level. Patrick Bridge has made this point well. Those at the community level have the most incentive to take action and to get the plans right. Organized mobilization of individual citizens is a critical part of the solution.

The National Academies have said that America's first line of defense is the first responder community, meaning the local police, firefighters and emergency medical professionals. But I'd like to push our collective thinking a little further in this regard. I'd like to suggest that there's a line of defense in front of these professionals – that the first line is <u>us</u>. <u>Us</u>, as an alert cadre of private citizens and local businessmen, who are in some cases the infrastructure owners and operators. We, as citizens, are really the front lines. We are the first layer or line of the defense and in some cases, the offense… the first to interface with the enemy or deal with whatever the situation or catastrophe may present.

Terrorists bring the battlefield to the local level. Terrorists creep around the edges of where we live and work. To use a military intelligence analogy, terrorists are like submarines. They hide undetected and move close to our critical systems. Eventually their object is to destroy them. Grass-roots participation, grass-roots alertness and protections are the best way to strip away the sanctuaries of the terrorists. The following quotes from terrorist literature point to the importance of local level preparedness. From Hamas: "If you are hungry, it is foolish to hunt a tiger when there are plenty of sheep to be had." From Bader Meinhoff: "When we have a free path, we go forward. If we meet an obstacle, we go around it. When the enemy is unprepared, we surprise him. If he is alert, we leave him alone. If the object cannot be overcome, we retreat." It is apparent that these people are looking for the chinks in our frontline protection. The more we're able to develop a unified culture of preparedness throughout our society, the less able they'll be able to hurt us.

The Homeland will be secure when our hometowns are secure.

Later this afternoon you're going to hear from Greg Saathoff, a psychiatrist and expert on duress from the University of Virginia. About two years ago he sponsored a panel of experts to look into the question: why have there not been Palestinian style suicide bombings in the United States? There were two basic reasons that emerged:

(1) The ferocity of our national response to 911. Al Qaeda did not expect that the U.S. would respond so forcefully. (2) The second reason is very interesting. The fact that American citizens took action in situations such as United Airlines Flight 93 and Jose Padilla's bombing attempt have had a definite effect on terrorist effrontery. The efforts of individual American citizens are very, very important and are having a decided deterrent effect, according to Dr. Saathoff.

Again reinforcing Mr. Bridge's comments, Dr. Baker made the point that we need to stop looking to Washington for critical infrastructure protection. The federal government is not organized, manned or equipped to manage operations on the local level. The federal government's role is an enabler of local response. It needs to do a better job to provide incentives for private engagement. But there is a growing problem that needs to be checked. A culture is developing within the state and local governments that looks on DHS funding as an entitlement. The federal government simply cannot spend its way out of this.

Assessments are very important part of the local effort for two reasons. The first reason is to understand what's out there, and how the systems work. James Madison University is doing local infrastructure assessments and finding that local public works folks don't have a full grasp of what their systems are. We're mapping networks, manholes and lines that didn't previously show up on system blueprints. This is a real problem. The government is trying to regulate systems they don't understand. We don't understand them at the local level. The second reason assessments are important is to understand how systems may fail and what the consequences of those failures would be.

In Dr. Baker's former position as the assessment division director at the Defense Threat Reduction Agency (DTRA), he was involved in assessing and protecting over 50 critical military sites. Many of the techniques and lessons he learned apply to critical civilian infrastructure systems. During his tenure at DTRA, Dr. Baker saw the same problems over and over again at the sites he assessed. Some examples include single point vulnerabilities inherent in co-located mission-critical systems. In many cases primary and backup systems were in the same room. Assessments revealed conduits or trenches where water, electric and communications lines were installed together. Unattended rear entrances, loading docks were common. We see exactly the same types of problems in the civilian infrastructure. It will be important to pay attention to the lessons from the assessments of DoD facilities.

People automatically assume that protection is going to be very expensive. It doesn't come free, but a lot of the most effective fixes we saw with military facilities were low cost procedural fixes. Steps such as adding or repositioning fences, changing car and foot traffic patterns, blocking windows into critical equipment rooms, and removing exploitable information from websites greatly improved security at different at critical military sites.

Local citizens need to know what the likely targets are.

Obviously we can't protect everything. It is commendable that DHS is adopting a risk-based priority allocation formula. But, in addition to national priorities, we need local assessment criteria, goals and metrics. The magnitude of the assessment effort in terms of sheer numbers of sites to be assessed will require the involvement of local agents.

At JMU we're addressing the problem as follows (in terms of local engagement). We are working with local government and businesses. We've begun performing assessments of local infrastructure. We have assessed the JMU campus, a local electric power grid, a local water system, and a local emergency communications system. We are enlisting the help of faculty and outside subject matter experts in these assessments. The new "NSRAM" network modeling software will soon be available to aid in our assessments. We have the idea that because there are so many systems out there that we will need to train local stakeholders to enable them to perform assessments. As we gain experience, we are planning to develop training packages on assessment approaches. We are currently publishing citizen's preparedness guides. In the future, we're planning to publish analogous self-assessment guides and training materials for local infrastructure service providers.

The above discussion reinforces the importance of education. We need an informed citizenry. They need to know more than the red-orange-yellow color codes. They need to know what threats are out there. We need to keep the threat out in front of the public because Americans have such short memories. Local citizens need to know what the likely targets are. They need to be instructed on simple procedural measures. Businesses should train their employees. The lawn maintenance crew is liable to be the first to see an incoming threat or hazard. The people working on your facility maintenance staff may be your most important asset in terms of real-time awareness and protection. Train your employees on what to watch for as they drive to work. General citizen awareness is important. Means include university/community college courses and continuing education seminars. Outreach should be enhanced by organizing town meetings to discuss protection needs and plans. A community education approach will create general awareness of infrastructure assurance objectives. Education is the key to developing the culture of preparedness we need at the front lines.

Remarks by Brashear

Remarks by Panelist Ron Raab, Professor, James Madison University College of Integrated Science and Technology.

Are you concerned about bioterrorism? People are forgetting about what happened in the fall of 2001 which included an anthrax attack here in D.C. I teach a freshman biology class of 30 students. Before I instruct them on pathogenic microorganisms, I ask how many of them are concerned about a bioterrorism event occurring. What is surprising is, on average, one third of them are not concerned and didn't think this could happen again. I know that all of you are concerned about such events or you wouldn't be here today. But, it is clear from my student's perceptions that as time goes on, concern slips. It's happening with funding agencies as well. And the development of preventive measures such as vaccines, therapeutics, and diagnostic equipment is stalled. And when the next event occurs we're back in the mode of playing catch up.

There is a history of bioterrorism in the United States. The anthrax events of 2001 are relatively fresh in our memories. In 1984, a bioterrorism event occurred in Oregon. An eastern cult spiked salad bars in a small town with salmonella. In the late 1930s the Japanese had a very, very active biological warfare program. They released plague infected fleas in China. They tested prisoners with various forms of biological agents. Going back in the history of America, in 1773 the British gave the Indians blankets infected with smallpox. So biowarfare and bioterrorism have been used for quite some time.

On the lists of known biological agents provided by the Department of Defense and the Center for Disease Control, the category that scares me the most is the one that is labeled "Category C- Emerging Diseases." The worrisome aspect of these diseases is we know so little about them. With known diseases we can try to develop vaccines, therapeutics, and diagnostics. With the emerging diseases, we can't. When SARS broke out just a few years ago, we did not know if that was a natural occurring or possibly accidentally released from a biological lab. Recently, scientists were able to recreate the 1918 flu virus. The fact that this is possible means that we might be looking at an intentionally created flu pandemic. It is possible to create hybrid viruses and bacteria. Dr. Ken Alabek, who used to head up the Soviet Union's bio weapons program, indicated that his organization developed hybrid Ebola smallpox virus. It is the unknowns that are of highest concern.

Plague is another highly lethal and communicable disease. Yersinia pestis or plague is very common in the western United States. In fact, less than a month ago a woman contracted bubonic plague in Los Angeles. In the western United States it is very common. But what happens if someone develops a strain that is antibiotic resistant? Our main defense is antibiotics. It is not difficult to genetically engineer a strain of plague that is resistant to antibiotics. Antibiotic-resistant strains of other diseases could also be genetically engineered, including tularemia, anthrax, and plague – all prone to evade our immune systems.

Why biological terrorism? It's relatively inexpensive. There is a U.S. Army study entitled, "The Relative Cost of Terrorism," that indicates that, based on the cost of producing mass casualties per square kilometer, biological weapons are the least expensive. Probably many of you have brewed beer, made bread, or fermented wine. All of these processes use microorganisms. You were using basically the same technologies that are needed to grow organisms for bioterrorism purposes.

Biological weapons are very different from conventional weapons that go "boom," and produce instant casualties. They are also different from chemical terrorism where an agent is released, you have casualties and you deal with it in a linear progression. A biological terrorism event can happen thousands of miles away and the explosion not occur until a week or two weeks later. I like to use the following example with my students. We have a group of students over in London studying. They are flying home from Heathrow Airport. As they walk through the airport there is a biological release of a communicable agent, such as smallpox. They walked right through it, so they've all taken it with them. Less then 16 hours later they are sitting on our beautiful quad there at James Madison University enjoying a nice day like today, intermingling with other students and faculty. A few weeks or ten days later, people are starting to get very sick, not just at James Madison University, but all over the world. The people that walked through Heathrow may have ended up in Egypt, Japan or anywhere in the world.

Smallpox is thirty-three percent fatal. We do have a vaccine for it. But the critical question is, "do we have enough vaccine?" And do we have it located in strategic places? If an aerosol release was to occur, 50 to 100 cases would generate widespread concern. There is a good chance that panic would ensue, not just locally, but world wide. The reason is that smallpox has been eradicated. So if we see even a few cases cropping up, we know there has been an intentional release. The United States has conducted exercises simulating smallpox outbreak scenarios. One of these, Dark Winter I, had particularly serious consequences in terms of the breakdown of governance.

Some of the more dangerous agents are Ebola, tularemia, plague, and anthrax. We actually had an Ebola virus outbreak in Virginia, not far from here. Fortunately the Ebola-Reston 1989 virus was nonfatal to humans. Only primates were affected. Tularemia is bacterial and it doesn't take many organisms to infect. Ten organisms and you can become very, very sick. Last summer our porta-shields on the mall in Washington picked up tularemia. It was inconclusive whether this was an intentional release or naturally occurring. At the time of detection, we hadn't had much rain dust was kicked up by exhaust vents. Tularemia is a naturally occurring soil bacterium. The plague is easily aerosolized. Pneumonic plague is communicable – it can be spread from person to person. There is no known vaccine for it. There are some in clinical trials against pneumonic plague under way, but vaccines have not been approved or released.

Before October 2001, to my students, Anthrax was the heavy metal band. After the letter attack of October 2001, we learned about the disease through the press including images of the bacterial strains, x-ray pictures of infected lungs. There were twenty-two cases and five deaths. The attack caused much of panic here in the D.C. area, and it costs a lot of money to mitigate. In one anthrax scenario a theoretical aircraft released 110 pounds of anthrax spores over an urban area in Northern Virginia, Maryland, and D.C. Total predicated that 5,250,000 people would be infected. The number of people dying without treatment totaled 100,000. Anthrax is not communicable; it's like the chemical release, only it takes a little while for the effect. The known treatment is antibiotics. The cost for antibiotics is would be $26.2 billion per hundred thousand people.

Now my fear is after talking with some of my freshmen students and members of the general public that we've hit the trailing edge of public interest mentioned by George Baker. As the concern fades away, so does the research priority and medical interest. Hopefully, forums like this will sustain interest and keep the research going. Regarding biological warfare, an important source of information are the World Health Organization projections.

We don't have the medical infrastructure to deal with biological attacks. There would be an overwhelming surge of people into the hospitals. Fairfax Community Hospital conducted a survey of their hospital staff and 25% of them said they would not come into work if there was a biological event. So in these surges we can expect to have fewer hospital staff due to illness and attrition. In addition, hospitals do not have enough respirators to deal with biological attacks. In a typical hospital, about 80% of the respirators are in use. Should we begin to stockpile respirators and other necessary treatment infrastructure and drugs?

I'd like to present a concept that is described by the acronym, SMELT. A smelt is a little fish and like most fish you want to have it fresh. If it gets out of date it stinks, it rots, and it's no good. My point is we need to keep current on the five areas identified by the acronym: Scientific, Medical, Education, Logistics, and Tactics. With scientific research we develop better medical treatments, diagnostics, vaccines, therapeutics. Medical countermeasures include vaccines. We don't have vaccines stockpiled and, in the case of plague, no vaccine exists. The anthrax vaccine requires many injections – 5 or 6 injections within the first year and then a yearly booster. Education on scientific and community preparedness is also key. We need to educate our public in community preparedness and response to biological disasters. As has been emphasized, the first line of defense is often members of the public on the scene, knowing how to help. At James Madison University, we are working very closely with USAMRIID, United States Army Medical Research Institute for Infectious Diseases. Our students also work at the local level including our emergency command center. They also work with the emergency response or health care providers in the community.

An important tactic is early warning through integrated defense. In this regard a strong intelligence program is important to have a good basis for advance warning. We heard earlier if we have enough forewarning, we can take steps to be prepared. There are many intelligence gaps. Trying to reduce the unknowns by determining who has biological agents and how much is very important.

Regarding education, at James Madison University, we are working very closely with the U.S. Army by taking their courses and turning them into civilian courses to prepare first responders who will be involved in command decisions when outbreaks occur. We want first responders to understand the technology and be able to make decisions on what to do tactically and logistically. We also have our students integrated into the research program at USAMRIID on vaccine development, diagnostics, and therapeutics. The benefit to USAMRIID is that we help to bring things to a quicker resolve. We have also saved the government considerable money since our rates are much lower than commercial laboratories. Some of the experimental vaccines we've developed are now being tested against both anthrax and plague.

I will end with this question: is the U.S. prepared? Since I am originally from California, I have an earthquake preparedness kit in my basement. But we also need to take personal steps to be prepared for biological and chemical outbreaks. There is a trail out on the West Coast called the Pacific Crest Trail, goes from the Mexican border to the Canadian border. There's a monument at the Mexican boarder with the inscription, "Prepare for the worst, hope for the best." Thank you.

Remarks by Tollar

Featured Speaker

Mr. Michael Lowder, Deputy Director for Emergency Response, FEMA

Mr. Lowder expressed his thanks for the invitation to speak and extended greetings from DHS Secretary Chertoff and acting FEMA Director, David Paulison. Chief Paulison is in Florida today meeting with the State officials in Florida as part of the preparation for this coming hurricane season.

As this morning's speakers indicated while covering a wide range of topics, we face a large set of threats from hostile nation states, terrorist groups, pandemic influenza outbreaks – including human and naturally caused disasters. It is very essential, it's critical, that we take opportunities like this to share ideas and to share lessons learned so that we can expect to benefit from the opportunities and experiences of others. This enables us to better prepare the nation to deal with potential events and to protect the people as well as the infrastructure.

Mr. Lowder was pleased to hear several morning speakers emphasize the need to prepare… the need to be ready. We must do that; we must be ready at all times. We must be properly positioned to prevent, protect, respond to, and recover from all types of hazards, whether natural or manmade. Over this past year, we at FEMA have had lots of opportunities to learn lessons from experience concerning how disasters impact individual lives, the nation's infrastructure, and what we must do so we are better prepared to respond to and care for people in the future. It's essential that we all have a strong organization both within FEMA and Homeland Security so that we are able to do this very effectively – and to work with our state and local partners, the private sector voluntary organizations to have a comprehensive plan and comprehensive program to meet the requirements of future challenges.

To say that 2005 was a challenge to DHS and to

FEMA would be an understatement. It's been a year of change and challenge. The year has been historic in that we faced situations and events that have never been seen before in this country. It's challenged our resources to the breaking point. At the same time, it has given us many, many opportunities to learn and to make changes; to learn lessons so that we're better prepared for the future. Katrina was a catastrophic disaster (we'll talk more about that in just a minute) but it is not THE catastrophic event. There are many other threats that we face that can make Katrina pale in comparison and we must be prepared to meet those.

This presentation will address some of the things that we at DHS and FEMA are doing based on the lessons that we have learned and discuss some of the preparations that we are making to meet what has been forecast as another record breaking season. The department is taking on a much more aggressive preparedness posture. DHS is an all-hazards department focused on the full rang of capabilities to prevent, protect against and respond to acts of terrorism and all other disasters.

Because we found that we were not as prepared as we need to be, DHS has implemented a structure and strategy to bolster preparedness efforts in three fundamental ways. First, the department has consolidated all the preparedness activities into a new Preparedness Directorate. Secondly, we've undertaken an effort working with our state colleagues to review the emergency plans of all major American urban areas, focusing on their level of preparedness as well as specific activities such as evacuation planning. Third is the funding for these preparedness activities based upon risk. The national preparedness goals and the target capabilities list will help form the standard to help fund the future state and local preparedness efforts.

DHS is also undertaking a number of organizational reforms and program changes, all designed to capitalize on the lessons learned and to better posture the department for the future. There are several key themes driving this organizational change. These include enhancing preparedness, strengthening security, enhancing transportation security, improving information sharing, and strengthening FEMA's operational capability. FEMA has undergone what's been called a retooling and rebuilding for the 21st Century.

The 2005 hurricane season resulted in many, many, many congressional hearings, IG Investigations, GAO Investigations, and nonstop media coverage. We have learned much from this scrutiny. The advice and criticism have been helpful to us in improving FEMA's operational capabilities. A major part of the improvements involves providing better tools for our people. Retooling has a focus on meeting of the needs of people – both the victims of disasters as well as the people that are responding to those disasters. It's a huge undertaking that is still in progress. It is being done in coordination not just within DHS, but with all related Federal agencies and the private sector.

> *Our job at FEMA is not to go in and take over; rather our job is to support the state and local efforts.*

Regarding FEMA priorities, Acting Director David Paulison has established four strategic focus areas:

1. Enhancing our operational capability
2. Building the capability and capacity for response to catastrophic disasters
3. Optimizing our flood insurance program and our mitigation programs
4. Transforming the FEMA organization to maximize employee performance.

Based on these strategic areas, the Response Division has outlined a number of priorities of its own. The response division in FEMA is the lead component within FEMA with responsibility of providing the immediate disaster response support to help our state and local partners. Contrary to what much of the media has suggested, our job at FEMA is not to go in and take over; rather our job is to support the state and local efforts. We deploy a number of teams to help do this including response teams, a search and rescue task force, a national disaster medical system, and mobile emergency response detachments. Other special teams include our hurricane liaison team, our domestic emergency response team, and the nuclear incident response team. We have a wide variety of other supplies and support equipment to be used by the state and local folks as well as the federal responders. Our priorities are to improve our teams and our response capacity, to improve our logistics capabilities, to enhance our catastrophic disaster planning, and to enhance our disaster work force.

Along the Gulf Coast, 1.5 million people were evacuated. Two hundred and fifty thousand homes were either destroyed or heavily damaged. Over 1,300 people lost their lives.

To improve our teams and response capacities we have been working with all the other federal agencies to do what we call prescripted mission assignments. We use the term "mission assignment" in FEMA to denote a work order that we give to another federal agency. Under the Stafford Act we have the authority and responsibility to task other federal agencies to provide support to the overall disaster response based upon the state and local needs and requirements. We do this through the mission assignment. We have reviewed and analyzed all of the mission assignments that we have given in the past to assess commonalities. We have developed a list of most used mission assignments and   prescripted those so that they are in the box and ready to go.

We have worked with the Department of Defense and we now have or are assigning a Defense Coordinating Officer and support staff to each of our FEMA regional offices. Including a Defense Coordinating Officer and their respective staff in each of our regional offices has enhanced our day-to-day planning and coordinating with the Department of Defense. We're implementing new response teams designed to deploy to the incident scene, work directly with the local incident commander, and provide direct support to them in conjunction with the affected state.

Relative to the upcoming hurricane season, we've enhanced our "battle books" for hurricane response including our concept of operations and our national and regional operations and procedures. We've worked tirelessly to improve our logistics capability. We have increased our stocking levels for commodities and disaster supplies. We've undertaken a strategic review of the locations of all of our disaster logistics centers and warehouses. We're implementing a new system of what we call "Total Asset Visibility" to allow us to better track the movement of disaster supplies and commodities and teams and other personnel. We're enhancing our catastrophic disaster planning and initiatives by developing field hospital prototypes for deploying an enhanced medical capability to meet surge requirements.

We have been working with other federal agencies, specifically the Department of Health and Human Services to plan for pandemic influenza contingencies. We're involved in more robust specific planning working with a number of high risk areas across the country to include the New Orleans, Southeast Louisiana, the New Madrid Seismic Zone area, and south Florida to initiate more detailed planning for a potential catastrophic event. New Orleans event has provided much insight into required planning for large scale disasters. We are applying this insight in the other areas of the country relative to category 5 hurricane and earthquake risk areas.

We are also enhancing our work force. On the scale of federal agencies FEMA is very small. At present we have about 2,100 people. We also have what we call our Disaster Reserve force of 4,000 people on-call. We've undertaken a significant effort to retrain our Disaster Reservists so that they are better equipped and able to go out and provide support following a disaster declaration.

There is a “Story That Hasn’t Been Told” behind the 2005 hurricane season. Most people know that the 2005 season was the most significant season in history. There were twenty-seven named storms and fifteen hurricanes. Three hurricanes were category 5 and twelve were tropical storms. Hurricanes Katrina and Rita were two of the most intense hurricanes ever recorded in the Atlantic. Hurricane Katrina was the largest natural disaster that this country has experienced. It affected an area of approximately 90,000 square miles… the same surface area as Great Britain. Along the Gulf Coast, 1.5 million people were evacuated. Two hundred and fifty thousand homes were either destroyed or heavily damaged. Over 1,300 people lost their lives.

In a one week period after Katrina, we delivered 580 truck loads of Meals Ready to Eat were provided – that’s over 11 million meals. We provided over 1,600 truck loads or 30 million liters of water. During the same period we delivered over 2,000 truck loads or 81 million pounds of ice.

In advance of the storm, FEMA pre-positioned 1,400 people in the Gulf Coast. Prior to land-fall, we pre-positioned over 1,200 tractor tailor truck loads of commodities in the Gulf area. In the first six days after Katrina’s land-fall, more truck loads of supplies were delivered to Katrina victims than in the entire seven weeks following the four hurricanes that hit Florida in 2004. Over a seven week period during to 2004 Florida hurricanes, we provided 425 truck loads of MREs (Meals Ready to Eat) which equates to 8.5 million meals. We delivered over 1,900 truck loads or 31 million liters of water to disaster victims. In addition we provided over 1,300 truck loads or 50 million pounds of ice to the disaster victims in Florida.

In a one week period after Katrina, we delivered 580 truck loads of Meals Ready to Eat – that’s over 11 million meals. We provided over 1,600 truck loads or 30 million liters of water. During the same period we delivered over 2,000 truck loads or 81 million pounds of ice. These numbers set a historical record for FEMA commodity delivery during a single disaster. And our numbers don’t include meals that were provided by the Red Cross, the Salvation Army, and the other voluntary organizations. In response to the 2004 Florida hurricanes, we delivered a total 3,700 truck loads of commodities to disaster victims. In 2005, which includes Katrina, Rita, and Wilma we delivered over 54,000 truck loads of commodities to the victims of the Gulf Coast hurricanes.

The Natural Disaster Medical System played a significant role in the 2005 hurricane disaster response. The Natural Disaster Medical System is supported by several federal departments including the Department of Homeland Security, Health and Human Services, Department of Defense and the Veterans Administration. Each department has specific roles and responsibilities as part of the system. FEMA’s responsibilities include the medical teams, the disaster medical assistant teams, and the veterinary teams. During the time period between Katrina and Rita, our NDMS teams treated over 165 thousand patients. We deployed over 5,000 NDMS professionals including doctors, nurses, pharmacists, radiologists, and EMTs. Over 15,000 animals were treated by our veterinarians. Within our Urban Search and Rescue System, we have 28 task forces. All 28 were deployed during Katrina and Rita – a force of over 2,500 search and rescue personnel. These units rescued over 6,500 people.

Record numbers of people were evacuated and rescued during Katrina. Evacuations were conducted by FEMA, DOT, DOD, FAA, Transportation Safety Administration using buses, trains, boats, and by air. We conducted the largest domestic civilian air lift in our nation’s history – over 22,000 people were evacuated by air within a 48 hour period during “Operation Air Care.” The 2005 hurricane response included the first deployment of U.S. military forces in the U.S. on U.S. soil since the Civil War. Over 72,000 active duty, reserve and National Guard personnel were deployed and responded to the hurricanes. The Department of Homeland Security components which include the U.S. Coast Guard, ICE, Customs and Border Patrol and others rescued over 40,000 people during the course of the storm.

There were over 600 thousand people that required sheltering and care after the storm compared to just 180 thousand after the 2004 hurricanes in Florida. Six hundred thousand people were moved across the country. States and local jurisdictions opened their doors, received evacuees, integrated them into their communities, and provided care and support for them. And all of this was done on an un-preplanned adhoc basis.

There were several key lessons learned. While the response to Katrina was unprecedented, it was not without flaws. Katrina has given us a precedent to measure against as we improve our plans and capabilities. We focused on identifying and learning both from what went well what didn't. We recognize the difference between learning lessons and acting on what we've learned. Based on lessons, we are making doctrinal, policy and procedural changes to ensure that we co-locate all of our key decision makers from the local, the state and the federal level to facilitate sharing information, command and control. We are taking steps to ensure that we can support them by having pre-positioned and ready to operate communications assets to enable awareness of what's happening on the ground, control of response actions, and feedback on the effectiveness of those actions. Our communications takes into account the need to have appropriate coordination and access to the key Department of Defense Decision Makers that are working in support of a disaster response.

We have designated locations where we are going to pre-position key assets, commodities and staging areas. We are enhancing our ability to alert the public of impending situations through our Emergency Alert System. We're working with the States help them pre-contract their own disaster response resources and commodities. We're also enhancing our ability to work with the States to help them develop more comprehensive emergency plans and to help exercise those plans. We're taking steps to enhance and improve the delivery of disaster assistance to victims.

Improvements that will be in place for the 2006 include enhancements to our partnerships with the States as well as improvements to our contracting capabilities and agreements to make sure that we have sufficient stock piles of commodities. We are upgrading our communication facilities, both fixed and mobile. We are pre-designating and we will be pre-positioning five leadership teams across the coastal areas to ensure that we have a much better coordination and cooperation with our State partners. We're assigning these teams to the Gulf Coast, to Florida, to the Northeast, the Mid-Atlantic, and to Texas. We're placing Defense Coordinating Officers in each of our ten FEMA regions. We are prescripting all of our mission assignments with the Department of Defense so that those can be executed in a much more expeditious time frame. We're enhancing our communications capability by moving into newer technology. We're making sure that we have effective interoperability with our communication so that what we have will work with the State and with local jurisdictions. We will have many of the same tools being used by the news media to enhance our ability to collect information about the situation.

We are expanding the scope and capabilities of our Federal Search and Rescue partners. We're activating more assets and will activate them sooner, placing them closer to the anticipated land fall. On the disaster victims side we are working closely with the American Red Cross to develop better methods to identify and assist evacuees. We're enhancing our capability to register disaster victims, so we have the capacity to register up to 200,000 per day. We've moved away from a telephone-based system and will now use an expanded, internet-based registration system. We are coupling this with mobile registration intake centers that can be moved into communities and co-locate with care shelters to help victims register more quickly. We are instituting a system of identity checks as part of the registration system to cut down on fraud. We are tripling our capacity to do home inspections from 7,000 to over 20,000 per day. We are enhancing the process to determine an applicant's eligibility for FEMA's assistance programs. We're enhancing our ability to support local jurisdictions with debris removal contracts. In the past this has been a FEMA-Army Corps of Engineers task. We are changing the system to facilitate local jurisdictions' contracting at the local level.

It has been a very challenging number of months in the wake of hurricane Katrina at all levels from the victims, to the local communities, the volunteer agencies, the States, to the Federal Government. FEMA will continue to implement significant additional enhancements to strengthen the nation's preparedness and our ability to respond and recover from disasters. We do this by working together so that we are prepared as a nation to protect, respond, and recover from catastrophic events.

Panel Three – Response

Ken Newbold, James Madison University (Moderator)

Remarks of Panelist Joshua Barnes, MSA, Inc.

Mr. Barnes addressed "Humans as Critical Infrastructure." Planning is an essential part of any response operation. In our planning, we need to think of humans as critical infrastructure. This heightens the awareness that communities and organizations, as complex systems, require specific attention to protect them against disruptive events.

Why are humans a critical infrastructure? They play critical roles in the function of traditional physical infrastructures. People are dependent on critical infrastructures. And the infrastructures are dependent on people for design, construction, repair, improvement, and innovation. Humans are critical in the communication among critical infrastructures. As an example, consider the importance of the communication between the manager of a local water plant and the manager of the servicing electric power system. Humans are an infrastructure in and of themselves based on the way that communities and organizations develop and function. Organizations are inherently complex.

There are four principal elements of the human infrastructure:

1 **Academia.** Academia is responsible for providing the highly skilled labor for a knowledge-driven economy. They provide education and training for the people who run critical infrastructure systems. Academia can serve as a very effective intermediary between industry and government.

2 **Government on the federal, state and local levels.** Government organizations create the policy environment governing the operation of critical infrastructure.

3 **Non-government organizations.** NGOs act as a catalyst for attracting funding and training responders. Many of these are volunteer organizations that play an important part in preparedness and response.

4 **Industry.** Clearly private is an important part of the infrastructure since most of the physical infrastructure is privately owned. Their role is vital.

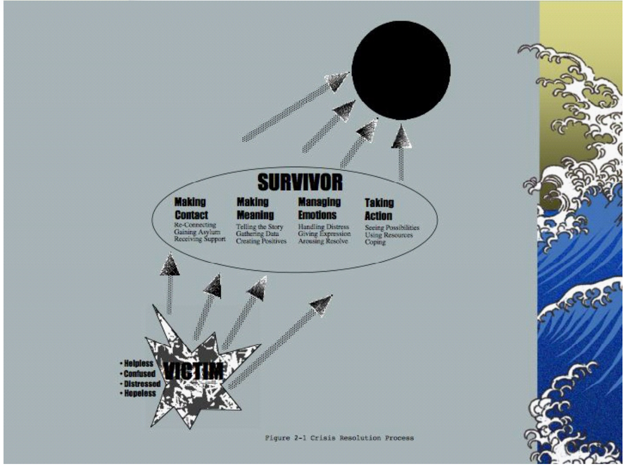
COOP (continuity of operations) planning is oriented to sustaining human infrastructure. At the federal level, COOP planning is guided by Federal Circular 65. COOP events are unpredictable. Organizations should adapt an all-hazards view so that it will be possible to adjust to any contingency. COOP requirements at the federal level include the ability to have essential functions up and running within 12 hours after a catastrophic event. These essential functions must be sustainable for 30 days or longer.

How does COOP work? Organizations identify their essential functions that must be sustained in the event of a given catastrophe. Organizations also identify their essential personnel along with the equipment needed to enable essential personnel to execute their functions. Vital records must be identified. At the community level, fire fighting would be an essential function.

Figure 21

Figure 22

Figure 23



COOP is essential to critical infrastructure assurance. COOP is a way of planning to prepare organizations so they know clearly, before an event, what needs to be done, how it needs to be accomplished, and by whom. Logically, better planning and preparedness yields more effective response. As a critical infrastructure, the human component needs careful planning and practice to reduce the response time.

Planning must start at the community level. All disasters are local – first responders come from the local community. Planning begins with local leadership in government, business, the medical community, the legal community, civic organizations, faith-based groups, not forgetting the general public in the hopes of creating a faster, more effective response. Much time and hard work are required. But addressing the human infrastructure specifically in the planning process will have great benefits in responding to and recovering from catastrophic events.

Remarks of Panelist Dr. Lennie Echterling, Department of Psychology, James Madison University

One of the advantages of going later in the afternoon in a conference such as this is the opportunity to build on ideas that people have already presented. In particular, I'll be building on points that Josh Barnes has made because, as a psychologist, I'm very interested in the human infrastructure. We've also talked about "grass-roots" – that's been a common word today, and I want to emphasize that people at the grass-roots are psychological resources. When we talk about grass-roots resources we're talking about parents, citizens, teachers, clergy, and volunteers who have opportunities to assist individuals hit by a natural disaster or an act of terrorism. They're not victims – they are survivors. We have also been discussing the term "resilience" many times today. And in terms of an infrastructure (including technology and businesses, economics, and so forth) I'm also interested in the personal resilience – the psychological resilience of individuals. I will be emphasizing this idea in my brief remarks.

I'll be discussing infrastructure as a "Commons," as a psychological sense of community. Richard Little introduced this idea earlier. With that in mind, coming from the field of psychology, we have spent much time understanding disorders, dysfunctions, and negative conditions. Psychologists study negative emotions including anxiety, depression, aggression, etc. This study has been helpful for people with those particular needs.

Positive psychology is a fairly recent development and is becoming a focus of many studies. We're realizing the importance of looking at the whole human experience and in addition to looking at the problems, including attention to the strengths, the character, and the potential that humans have. For example, one can type in the word 'anxiety' into a psychological data base and immediately get thousands and thousands of hits of psychological studies that have been studying facets and nuances of anxiety. A search on the word 'hope' yields far fewer. Type in the word 'compassion' or even 'resilience' and one sees even fewer.
Positive psychology has been an important influence in the field of crisis intervention. We are beginning to look at individuals in crisis situations not as passive, pathetic victims who are dealing with communities that are totally destroyed; but rather to see them instead as having possibilities and potential and strengths that we can work to enable them and facilitate a resolution process. This leads to the concept of personal and community resilience which we've also been discussing in terms of infrastructure.

Many people come away from these experiences being involved in something bigger than themselves, with a greater sense of maturity, a larger appreciation for what life does have to offer, and a recognition of their sense of community.

Even if you're not a psychologist, you're very familiar with the term "PTSD," or post traumatic stress disorder. It's important to keep in mind that in epidemiological studies after disasters, the majority of individuals that have been involved in crisis experiences do not develop that particular disorder. In fact we're finding that many of them, as we do follow up studies on their experience, have experienced PTG or "post traumatic growth." Many people come away from these experiences being involved in something bigger than themselves, with a greater sense of maturity, a larger appreciation for what life does have to offer, and a recognition of their sense of community.

There's an interesting study that was done by

Figure 24

Figure 25

James Pennebaker who is a social psychologist at the University of Texas. As he was analyzing oral communications taking place in a certain community, a public trauma took place. It was not planned or anticipated, but he continued on with the study. He found that our communications in just everyday contact with others changes in some very subtle, unconscious ways. One of those changes was that the use of the word "I" went down 12 percent from before and after this public trauma. The use of the world "we" – the personal pronoun that communicates something bigger than ourselves – went up 135 percent. There's something going on here that represents evidence that community resilience with that social fabric that doesn't have to be torn – that in some ways may even be strengthened.
Here's a drawing that a child did after a natural disaster and its very typical of children's drawings in situations where they want to give expression, to take the raw experience of the catastrophe that they've encountered and experienced, and put this into the nonverbal story of a picture. See Figure 21

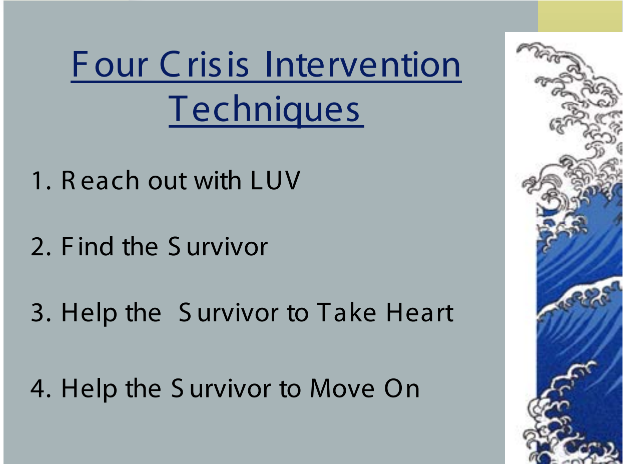
And so we get a powerful imagery of what happened. To this story of crisis we're now inviting children as well as adults to give expression to their resilience. I asked this same child if he could also draw me a picture that would express some lesson that he'd learned from his experience – something that could be helpful to another child who might be faced with this type of catastrophe. In response, here is what this child drew. It says 'You will be surprised what you can live through.' See Figure 22

It is important for individuals and communities to recognize and give expression to their resilience, to acknowledge they have lessons that they've learned and they are making it through what has become a story of survival. Human beings are meaning-makers. Who we are is a result of the stories that we create. Our national character, our community history is made up of a collage of collective stories. We need to be careful about what these stories say about us. Because they can become expressions of frustration, victimization and passivity, or they can become expressions of vitality, hope and resilience. The latter response becomes very fruitful in making sense of and recovering from catastrophes.

See Figure 23
The chart above provides an overview of the psychological process that goes on in times of crisis when a catastrophe has hit as depicted in the lower left hand corner. People can be overcome by extremely tragic circumstances. We are all vulnerable. We talk about ways in which people may feel helpless, confused, distressed and even hopeless when tragedy strikes. What we find from interviewing people who have gone through personal or community catastrophes is that they immediately begin to go through a survival process.

There are four factors that seem to be important in promoting resilience and survival:

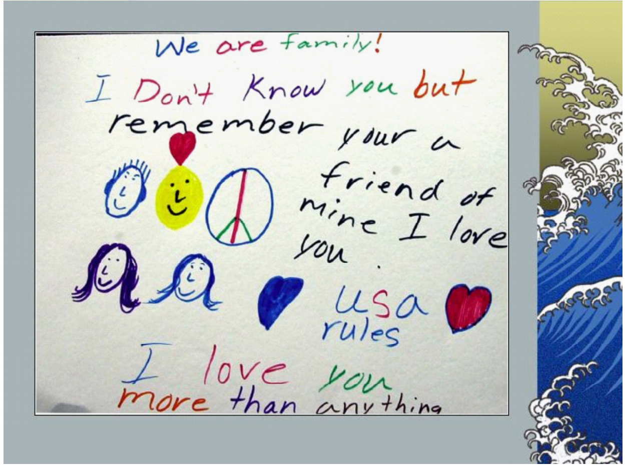
Figure 26



Four Crisis Intervention Techniques

1. Reach out with LUV
2. Find the Survivor
3. Help the Survivor to Take Heart
4. Help the Survivor to Move On

Figure 27



Support from community The greater physical and emotional support environment., the more people are able to come through the event at a higher level of well-being. In terms of making contact, we seem to have a need to reach out to others. Other panelists have used the world "interdependence' as they addressed different kinds of systems. Similarly, we as human beings are interdependent.

A psychologist by the name of Rime did a study involving interviews of individuals about recent negative or positive emotional experiences. He found that 95 percent of those interviewed shared their experience with someone else within 3 hours. It is important to facilitate this kind of communication following disasters. Panelist George Baker made the point earlier that the first responders are actually us. This is an important part of the "reaching out" process. Initially, it's not the trained technicians, the rescue squad, or the volunteers. The first responders are the parents, the loved-ones, the neighbors, the fellow members of the school, or church community that make a difference here.

"Meaning making" is an important part of the recovery process. Janoff-Bulman discussed this challenge that we have in time of crisis to make sense out of what has happened. Survivors need to fit their experience into their view of what's meaningful in life, to fit it into their religious framework and their view of themselves as well. It's a powerful challenge to somehow come out of a tragic experience being more informed and more aware about what's important in life and to create a meaningful post-disaster existence.

Figure 28

Managing emotions is a factor that we find very important here. Typically we think of emotions such as anxiety and fear and apprehension and depression. But in addition, we're finding that good predictors of well-being following crises are the presence of positive emotions. These are fostered by acts of compassion that we experience and share with one another. Another source of positive emotion is the humor that we often find ourselves enjoying including gallows humor. This helps us through tough times and gives us courage that we might not have otherwise experienced. Also, feelings of resolve make a difference in promoting a well-being and a positive resolution.

And fourth and finally, the taking action to restore our future. Part of our response has to be to enable people to envision a future once again – to begin to look at possibilities and to, as Emily Dickinson said, experience "hope – that thing with feathers" that helps us to transcend the crisis experience. I'd like now to share with you a couple of stories and vignettes that demonstrate the kind of psychological experience that goes on in the trenches. See Figure 24

This is my colleague, Anne Stewart from JMU, who is working with survivors of the tsunami in Sri Lanka. You can see here that just coming together can be a powerful psychological experience so that individuals feel that they're not alone – that others are reaching out to them.

The following chart is a picture of the destruction in Pascagula, Mississippi. It's the remains of a house. In addition to the address and other markings you see that the individuals who lived there decided to make meaning out of the experience and share a message with you that you may not be able to read, but it says "do not allow Katrina to steal your joy." See Figure 25

This is an example of the devictimizing strategy that many human beings have. We don't want to consider ourselves as passive-pathetic victims. Rather we want to see ourselves as people with hopes and dreams that we want to share with one another. Many of the grassroot groups that we've talked about – the CERT teams, the clergy, educators, first responders, day care providers, and parents – need information and training to make a difference.

Some practical crisis intervention techniques are shown in this chart. See Figure 26

These can be easily communicated to volunteers without the need for professional mental health qualifications. It is helpful to acquaint first responders with these techniques to make a difference as they help and encourage survivors to move on with their lives. See Figure 27

> *One assumption is that trained emergency personnel will triage people in the field. But people aren't going to wait.*

This was drawn by a child who was invited to participate in sending messages to the Pentagon and other survivors after 911.

The following chart illustrates a way we can help children to be involved:

We are developing a website that provides an electronic community forum where individuals at the local level can share their children's drawings, their stories, resources and other helpful information to make a difference in helping communities to come together to express their resilience. The picture above is a posting from that website. We've used pictures of children to make a calendar of stories of survival we've assembled as a way of expressing collective resilience.

> *Base disaster plans on what people are likely to do rather than what they should do.*

See Figure 28

In closing, here is the picture of a young child that we've encouraged to keep a journal of survival.

We ask them to relate how they've helped or made a difference, and what lessons they have learned about their own strengths and what's important in life.

As we address important issues concerning infrastructure and resilience, psychologists see this endeavor as an opportunity to get to the bottom line: the promotion of human well-being, human resilience, and human infrastructure.

Remarks of Panelist Mark Kirk, M.D., Department of Emergency Medicine, University of Virginia.

Dr. Kirk provided perspective on medical response based on his considerable experience. He currently works as an emergency physician at a level 1 trauma center. He is a medical toxicologist, involved in running a poison center that coordinates extensively with other emergency centers at the regional level. His entire professional experience has been in the emergency response environment. In the mid-1970s he served as an emergency medical technician and volunteer fire fighter. Since then, he has played many different roles in the response system, from top to bottom, including flying on EMS helicopters and being part of a medical disaster assistance team for hurricane response. Dr. Kirk provided lessons he has learned from a medical perspective.

Disasters are predictable in some ways. Maybe not where they're going to happen and not exactly what will happen, but there are some themes that run through every single disaster. We can predict recurring problems and the behaviors of people during those times. A new area in medicine and in emergency response in particular is called "evidence-based disaster planning." A lot of current publications in the medical literature are focused on this. One person, Dr. Eric Auf der Heide at CDC has published many different papers on this that have influenced Dr. Kirk's thinking and efforts over the last few years. His guiding principle has become "learn from the past." And one phrase that really stands out from Dr. Auf der Heide's work is "base disaster plans on what people are likely to do, rather than what they should do."

Over the years we've written many plans in which we told people what they should do. For instance, if we had a chemical disaster or any disaster, we directed everyone to wait at the scene until we arrived and took them to the hospital. And hospitals didn't feel they needed to be prepared to take people right off the street. But we've learned from the Oklahoma City bombing, Tokyo sarin attacks, and many other disasters, that people aren't going to wait. So we've changed our approach accordingly: plan based on what people should do to what they are likely to do.

The Tokyo sarin attack occurred at 7:55 in the morning with agent release in a crowded subway. The closest hospital, St. Luke's International Hospital was about a mile from the subway. Over five hundred people showed up in the first hour. At the University of Virginia emergency department, three hundred people in a day is a busy day. So five hundred in one hour is overwhelming. Complicating the situation, it took about three hours before the hospital was aware that the agent was sarin. During the initial hours, emergency responders had no clear idea of what the problem was or that it was even a toxin.

There were many lessons learned from this event. Dr. Okumura, one of the physicians present in the emergency department observed that in chemical disasters, poison information centers should act as regional coordinators of all toxicological information. He also recommended that police and fire departments, health centers, poison information centers, and hospitals need to form an information network. Dr. Kirk took this to heart. Since then he has devoted a significant amount of his time to setting up such an information network at UVA. One of the marks of the success of this network was that, even though Dr. Kirk's center is in central VA, at night the center was asked to cover South Carolina.

About 2:00 AM on January 6, 2005, a train carrying tanks of chlorine collided with another freight train and derailed in a small community, Graniteville, SC. A large toxic cloud of chlorine drifted over the community. The first call to the poison center was from a nearby resident – not from the hospital or the emergency response department. The resident said her eyes and throat were burning and it smelled like a swimming pool at her location. What should she do? Dr. Kirk's center immediately called the hospital nearest to the scene and asked what was going on there. They hooked the poison center up with the local emergency management people and Dr. Kirk started getting information on what the chemical could be.

Typical of all of these, just to illustrate the point, the same pattern that occurs in disasters is illustrated here. The local emergency responders initially said the toxic chemical was sodium nitrite. Then they changed their diagnosis to methanol. Based on the clinical symptoms they were seeing, the poison center was able to advise the hospital that the alleged chemical was not causing the victims' illnesses. It took over an hour to confirm that the toxic chemical was chlorine.

As EMS responders rushed to the scene, they described hundreds of people leaving the scene of the accident. Only one physician was on duty in the local Emergency Department in this small community hospital and he was taking care of nine critically ill patients. He said there were at least 100 in his waiting room. This situation is also typical and predictable – overwhelming numbers of victims will arrive in a short time while little information is available regarding the hazard.

One of the most critical things in a disaster is trustworthy information.

Dr. Kirk then asked the question, "Who are responders?" In his world, he focuses mostly on chemical disasters. But in disasters in general, who are the responders? We can list a lot of people. Dr. Kirk works with a lot of different groups. Stake holders are all over the place. All the way from state officials to federal resources, but we need to work our way down in the other direction to the public. And we've heard this over and over again throughout the day; the public is an important responder. Evidenced-based disaster planning, some of the practices and publications illustrate this point again and again.

There are a lot of assumptions in disaster planning. One assumption is that trained emergency personnel will triage people in the field. But people aren't going to wait. What really happens is the survivors carry out their own search and rescue, their own triage, and, whether they recognize it or not, a lot of the primary medical care. Trained personnel will triage and treat at the scene. But most survivors leave the scene – they bypass the emergency response system in general. And casualties don't arrive by ambulance. In Tokyo, the first cardiac arrest arrived by private minivan. Only 23 percent of the people came by ambulance. A lot of people walked or came by taxi.

There are three areas that Dr. Kirk believes are critically important. The first is planning and training. The second is information management. Number three is interoperability and relationships. There are many other areas but these are the three that need the most emphasis.

There are some challenges and barriers facing responders. We have a tremendous resource in our nation and those are the responders from all groups… the public, the Emergency Medical Services, the firefighters, and volunteer groups. Everyone is motivated to do the best they can. These organizations want to learn and they want to train well so they can do much better the next time something bad happens. A problem arises when we basically "carpet bomb" these people with too much information. Much of the information is unfocussed and overwhelms the trainees. They don't even know where to begin. There are too many "what ifs."

Dr. Kirk recently participated in a drill in which participants dealt with concurrent biological, chemical, and radiological events. There were so many different things coming in that people didn't learn anything other than it was a no-win situation; that they were going to fail.

We need to back up and look at common competencies that can be used in every single disaster – things that people need to know how to do. There is a useful analogy with a football team. It doesn't matter who your opponent is: you have to know the basic skills. Players need to know how to tackle, punt, block, and pass no matter who your opponent is. We need to boil down our training to that level. Most training includes overwhelming amounts of detail.

Another example is the training provided over several days in one of the communities where Dr. Kirk worked. Three full days of biological, chemical, and radiological disaster information was poured into everyone in the community. Not too long after this, we had an anthrax hoax where a letter was delivered to Planned Parenthood. The response was typical. We had flooded the first responders with so much information that the only thing they remembered about anthrax was that anthrax was bad stuff. There was panic at every level of the organization and community response. We provide people with a lot of planning information but we haven't done a good job of helping them sustain a minimum set of essential skills. We need to stop preparing for nebulous "what ifs."

It is important to consider our own communities. Every community is unique. Look at what are the realistic problems and vulnerabilities that are in your community and also what are your realistic capabilities to respond. If there is one community hospital with one physician at night, it won't be possible to deal with 500 people at once. Communities need to look at what resources they can muster during a catastrophe and where to go for extra help.

We often get inaccurate information, but accurate information may not translate to actionable knowledge.

Every piece of emergency response equipment that we purchase from this day forward and every minute of training for each person needs to have a purpose to it. We need to focus the training on know-how skills. It's important to have information and facts but it is more important to learn skills that can be applied and to produce trainees that are really good at what they do. "Execute" should be the watchword. Train people to execute the plan.

So how can we improve the response? We can build on available resources. A surprising thing about working at our poison control center is that people trust us to a large degree. We get calls about biological problems, radiological problems, rabies and even food poisoning. On Thanksgiving Day, if the turkey's been out too long, we'll get calls asking if it's still OK to eat it. The public trusts us about questions that are not in our realm of expertise. This is just one example of resources that already exist that people use. We should enhance those resources rather than creating new and unique things that people may not understand or use.

We need to treat information as a resource. One of the most critical things in a disaster is trustworthy information. In all disasters, useful information is at a minimum and confusion occurs because of conflicting information and rumors. We need to be very aware of how we're going to manage and use information. In this vein, interoperability needs to be addressed. Working in the field you soon learn that interoperability is not about buying a lot of technology, it's really about relationships. We need to build our technology around the relationships we form. It is most effective if the people who have established relationships through training are the same people who are present and offering information during a disaster. It is important that people hear the same voices that are teaching them prior to an event when they need help.

We spend a lot time teaching. We know that people don't remember a lot of what we teach them. It's surprising the next day, asking someone a question from a class that's just been taught. A lot of people are not able to remember. With this in mind, we advocate a concept called "just in time education" so that when something happens, it will be possible to provide "on the spot" refresher courses.

I am working on a project with James Madison University that is addressing the need for information about chemical risk in communities across Virginia. The project team has asked each community to answer 2 basic questions:

1. What are the most toxic chemicals stored, produced

or transported in our community?
2. Does our health care system and emergency response system have the knowledge, training, equipment, antidotes, and coordination to effectively respond to the toxic chemicals in our community?

Out of these questions comes a third question: Can we do anything to prevent an "accident" now that we know the community's greatest risks? To optimize emergency response, JMU and UVA are developing an integrated decision support system called "FALCON."

But what happens when individual plans collide and we lack a more unifying and organizing principle. If not panic, what is that? I call it "Planic."

I will close my presentation by highlighting important points concerning interfaces in response from a medical perspective. We need to develop new technologies in a way that involves the grass-roots responders. One of the successes of the FALCON project is that we've involved the first responder users in the project review process. We're asking them what they think about the product and how well it is addressing their real needs. The most sophisticated technology in the world is worthless if it doesn't address the needs of the first responders. Most people that work in EMS have no qualms about junking new, expensive technology unless they are involved early in the in the development cycle. This is especially true of communications and emergency management equipment.

Educators and developers of educational technology need to work at the grass-roots level. Don't ask too much of these people. They're already learning so many other things. Boil the information down to some very basic things they can learn. They're bright people but they're being bombarded from every direction. Be respectful of their time. Simplify to the basic competencies and concepts. Keep it relevant. If we want to have a trained response system, we need to incorporate these skills into things responders are going to do on a daily basis so that their skills are well practiced. We should not teach skills they must pull out of a bag when the big one hits. And we need to really look at the sustainability and retention of these skills. Finally, emergency planners, working with grass-roots responders, need to keep the plans simple. Think about execution. Complex plans are destined to fail.

We need to focus our response capabilities on what's most likely to happen. Once we are prepared for the most likely events, we can adapt to other unplanned events. We need to focus on communication and key relationships – a main part of training and planning is developing and exercising relationships. Drill with a purpose.

Remarks of Panelist Greg Saathoff, M.D., Director, Critical Incident Analysis Group, University of Virginia

Dr. Saathoff expressed his thanks to JMU, IIIA, and CIP Program. He began with a true story. Recently, he interviewed a man who woke up one morning; turned on the television; and as he was eating breakfast, he noticed that his country was being invaded. The invasion was beginning in the very city where he lived. He finished his breakfast, finished dressing, got in his car and drove to work. When he was almost shot by soldiers, he reversed course and raced back to his house. Safely inside, he thought to himself, "You stupid idiot – you saw on television what was going on in your city and yet you went out and put yourself at risk." This interview was one of the most striking and meaningful Dr. Saathoff has had. It demonstrates the important lesson that information at a time of crisis is not enough. This man had true and accurate information. As Dr. Kirk mentioned, we often get inaccurate information, but accurate information may not translate to actionable *knowledge.*

Certainly we have definitions of terrorism such as "attack of noncombatants with the intent to provoke fear." And of course, noncombatant response is a necessary part of drama of terrorism. To illustrate this point, I will relay a very recent personal experience. It is a cautionary tale.

I landed at Dulles Airport that afternoon and was struck by the situation he found. Usually, when passengers go into the international terminal, they go through customs and then proceed to the baggage claim. Normally it's a very routine event. Almost like the march of the penguins. People come up and go to the carousel and pick up their luggage. The bags are spit onto the conveyor and there's an attendant who stands at the base of the carousel where the bags emerge. They come out and the attendant lines them up. On this day it was different – there was no one there to line up the bags. As a result, the bags took on a life of their own. Luggage pieces were bumping and grinding as they went around the carousel. A number of pieces fell off. Four flights were listed on the carousel marquis. So there were people from 4 different flights waiting about four or five deep watching as the bags were falling. At this point an elderly airport attendant ran up and started furiously pulling the bags off of the moving carousel and throwing them into a pile that was getting higher and higher. The growing mountain of bags was a pretty remarkable sight; particularly when one of the bags came open. Next, a passenger came over and tried to assist the attendant. So the mountain of bags got bigger. Waiting passengers began shouting saying "Hey, what are you doing to my bags?" If baggage claim is normally like the movie, "March of the Penguins," this scene was more like Hitchcock's "The Birds." If not panic, there was certainly agitation. Finally, the woman next to me said, "well, maybe the bags are over there." And even though the flight was listed on the malfunctioning carousel, I took her cue and walked over to the next carousel where I found my bag stacked in another pile. I then walked back to the first carousel and mentioned to a fellow passenger that the bags from their flight were on the next carousel. The passenger responded, "But the sign says our bags are coming here." Undaunted, I proceeded to customs and found out the line through customs was now very long because of the problem with baggage.

This vignette illustrates a classic cascading failure situation. Why did this cascade occur? An investigative review board would not allow a situation like this. There's no way they'd allow this to happen to bags. There certainly would be liability concerns. I wasn't about to start grabbing bags and throwing them onto a pile. The scenario illustrated the results poor communication as well as flaring tempers. Each passenger had his or her own plan about what to do once the bags were retrieved. How is it possible for passengers to retrieve bags from a luggage carousel when there is no coordination and false information? We know that panic is extremely rare following natural or man-made disasters. Read the literature and you'll be reminded about this by social scientists.

We find that people can and do behave altruistically. But what happens when individual plans collide and we lack a more unifying and organizing principle. If not panic, what is that? I call it "Planic." Mark Kirk described the problem of "too much detail." A surplus of information, much of it wrong, results in paralysis. Social scientists are correct in asserting that we shouldn't call this panic. But "planic" is a big problem.

How do we address "planic?" It is helpful to consider a concept that expands on the concept of "shelter in place." Because "shelter-in-place" is a cellular concept, it is necessary, but not sufficient. The concept of "community shielding" is an effective alternative to mass evacuation. It builds on "shelter-in-place" because we know that people make their best decisions in safe and familiar environments and, conversely, they make their worst decisions in unsafe and unfamiliar environments. We call it "community shielding" because it is implemented community-by-community. The idea follows and builds on earlier presentations, and particularly Dr. Kirk's presentation about community hazmat preparedness as a community-specific phenomenon.

We call it shielding because shield is both a verb and a noun. As a noun it is a protector but in heraldry, it's also a symbol. Different shields indicate that people come from different tribes. So community shielding is when related groups get together and organize shielding for a temporary period of time. This requires a partnership.

We have done some research on this looking at some real events. During a chemical incident in West Helena, Arkansas, citizens, when asked to shelter in place, did not respond as directed. They got in their cars and evacuated. Similarly, during a biologic case involving a meningitis outbreak in Mankato MN, people didn't do what they were asked to do. Both cases reinforce Dr. Kirk's remarks.

A GMU/JMU/UVA study showed the greater the sense of attachment to the community, the more amenable citizens are to shelter-in-place. But, the willingness to shelter in place is not supported by stockpiling the necessary supplies. We surveyed 1000 people and found that 25 percent of the National Capital Region population have no food stored and 40 percent have no water stored. On the positive side, those surveyed were interested in learning more about their communities and how to protect themselves in their communities.

Looking at the issue of quarantine, we know this to also be a necessary but insufficient concept. While quarantine is enforced, the active, opaque, top-down, involuntary, and often communication poor community shielding procedure is not. By the same token, targeted evacuation is something that is very important and will need to occur in any of these events.

Spontaneous, uncontrolled evacuation is a problem to be avoided. It occurs when residents see an emergency event and their movement means, and direction of travel is unorganized and unsupervised. It is right out of Hitchcock. We might not choose to call it panic, but it is an absolute disaster. Anyone who has been on the Capital Region beltway knows that it is impossible to have a mass evacuation of this area – particularly if it is spontaneous and without any type of control. It progresses according to what I call the "evacuation escalator." Once it gets started, it's very hard to reverse.

In our study, we found that 48 percent of people could not shelter in place at home for even a week. Only 23 percent had arranged for a family emergency site. Some key findings:

1. While 84 percent of the population, in a dirty bomb scenario, would follow instructions to shelter in place, 15 percent of the population would leave immediately for a number of different reasons.
2. Of 25 percent who would leave to find or take care of children or adult family members, 71 percent said they would stay longer if assured loved ones were safe and cared for.
3. Of 6 percent who would leave for food and water, nearly 86 percent would stay for 48 hours or longer if assured food, water, etc. would be delivered to their home.

Our poll regarding citizen response to a smallpox attack while at home provided major cause for concern. If no instructions were issued to shelter in place, 36 percent of the population would say home. A very large fraction of those polled, 38 percent, would evacuate. 13 percent said they would continue their normal route. 5 percent would stay at another nearby location (family member's home).

We looked at sources of information and the relative trust that different kinds of infrastructure and networks would continue to work in the event of a terrorist attack. We live in a very optimistic region. 48 percent of the National Capital Region population feels very or somewhat confident that transportation systems will work. 58 percent believed that internet access would be possible. Here is the list:

<u>Citizens "very or somewhat confident" in the availability of services</u>

- 95% radio
- 84% health care facilities
- 77% local television
- 74% public water
- 70% home telephone service
- 62% highways
- 59% cable television
- 58% internet access
- 48% transportation

And most feel that the federal government has the responsibility to ensure infrastructure availability. Here are the most important findings:

- With no request to stay, 41 percent will stay home or nearby, 59 percent will evacuate.
- If they are requested to stay, 57 percent will stay, 43 percent will evacuate.
- If food and water are provided, 76 percent will stay.
- If children and family are to be safe, 81 percent will stay.

> *The three " I's" of the future are Imagination, Integration, and Improvisation.*

Community shielding is a proactive, voluntary organizing principle. It is a community based action to encourage and assist people to remain in their home communities if they are not directly in harm's way. It provides a safe, secure, comfort zone using existing resources. The goals are:

1. To enhance capabilities at the lowest level of government
2. To enhance readiness
3. To strengthen temporary and emergency support, and
4. To insure the continuity of government and operations.

I will close with a quote from Thomas Jefferson: "I know of no safe depository of the ultimate powers of the society but the people themselves; and if we think them not enlightened enough to exercise their control with a wholesome discretion, the remedy is not to take it from them but to inform their discretion."

Panel Four – Future Horizons for Infrastructure Protection

Dr. John Noftsinger, AVP Research & Public Service and Executive Director, IIIA, James Madison University (Moderator)

Our final panel looks to the future regarding how we can better engage the frontlines. Relative to this, a recent Defense Science Board report on strategic communication included the following quote that I believe to be apropos.

"To succeed, we must understand the United States is engaged in a generational and global struggle about ideas, not a war between the West and Islam. It is more than a war against the tactic of terrorism. We must think in terms of global networks, both government and non-government. If we continue to concentrate primarily on states ('getting it right in Iraq,' managing the next state conflict better), we will fail."

You can find it on the Defense Science Board website. It is clear that we are now facing a new type of war.

I am pleased to announce that Ken Newbold, Jack Wheeler, and I at the Institute for Infrastructure and Information Assurance have a new book coming out soon entitled "Understanding Homeland Security, Policies, Prospectives, and Paradoxes." In the conclusion of our book we point out that education, research, and technology working together combined with the new innovation movement in the nation are critical to realizing robust infrastructures for our future. The business of homeland security really is here to stay. Both small and large businesses are developing homeland security units. Vulnerability, threat, cost analysis have become important factors in many decisions. In our book we talk about the cockpit door issue. Before 9/11 we knew the cockpit doors were vulnerable. Now it seems like a no cost, no brainer to actually reinforce those doors. There are literally thousands of decisions government's must make concerning these vulnerabilities including threat, and cost analyses of what can be done.

The role of the media needs to be examined. We see this in both the wake of 9/11 and we see this in the wake of Hurricanes Rita and Katrina. In the media craze today, the full scope of the media's role must be re-examined. As I mentioned earlier, our country was founded on a very personal relationship between privacy and security. This is a delicate balance that government has had to strike from the founding of our country; the delicate balance between security and privacy on the political and personal levels. This has played out most recently in the NSA Domestic Surveillance Program. Congress is still debating the issue, obviously you are aware of it, so stay tuned.

There are many good ideas out there regarding infrastructure assurance. Massoud Amin of the University of Minnesota, who is also involved in Lynda Stanley's Infrastructure Roundtable with the Federal Facilities Council, emphasizes what he calls the "Public Policy Trilemma" – the interaction of economics, politics, and technological considerations that permeate all public debates. Yakov Haimes from the University of Virginia and others have talked about about the Three R's, Redundancy, Robustness, and Resiliency as the elements of infrastructure assurance. Most of us are familiar with the work of Charles Perrow concerning Normal Accidents. We've heard speakers all day today talk about the extensive and complex infrastructure and that a certain amount of failure is inevitable and should be expected. Systems that are tightly coupled are more prone to cascading failures. Perrow identifies three types of disasters: natural, accident, and deliberate. Due to the relationship between vulnerability and complexity, he predicted that we will be seeing more and more "normal" accidents. Perhaps our salvation will be the resiliency of the human infrastructure, as Dr. Echterling has explained. But humans often complicate and cascading failures as we've also seen. Humans continue to be the strong and the weak link in the system.

Our book addresses "fighting the last war." John McCarthy of George Mason University will speak to us later. John was involved with the Y2K mediation and worked in the White House at the time. If you recall, there was much concern in the late 90's about Y2K. During the same time period, Dick Clark and others were pointing to the vulnerability of our information networks so our attention was diverted to protecting against cyber attacks. So what did we get? We got jet airlines flying into buildings as flying bombs followed by an anthrax attack on Capital Hill; a biochemical attack if you will. Subsequently, our focus was on preventing malicious physical attacks. What did we get next? We got Hurricane Katrina and Rita, once again a natural disaster that blind-sided us. Michael Lowder talked about Hurricane Katrina. We're still totaling the damage but the lessons are clear about the importance of planning, communicating, transportation, health and the role of the media as well. Now national concern is focused on an Avian Flu pandemic that could rival the 1918 epidemic. So what the heck is next? We don't know, but that's the world we're living in.

I'll leave you with some thoughts from the close of our book. The three " I's" of the future are Imagination, Integration, and Improvisation. We should not underestimate the innovative capacity of our youth. That is why many of us work in higher education. We're delighted to be working with the young people as we help them learn and grow. Our country is blessed with the very, very smart and innovative capacity for our youth. We need to arm them with the latest technological skills and improvisational skills and also, integrative skills. And this is the best hope for our future. One of our earlier speakers, Josh Barnes developed the concept of humans as critical infrastructure. People connect and manage all infrastructures. Hence, we should focus on helping humans develop their natural decision-making skills and intuition. An important tool is simulation, incorporating the most recent gaming theory. We should take the video games that our kids love to play and use them as a way to train our infrastructure professionals of the future to help them to make better group decisions in difficult situations. Finally, we need to strike that balance between instilling confidence in the system and having them follow rules and procedures, but also allowing for them to use their improvisational skills. We need to do this because the enemy we face deals in the unexpected.

However we know a few things about the future. Our enemy is a hybrid, blending financial resources with the efficiency and brutality of organized crime motivated by religious fervor. Their attacks are focused on financial and symbolic targets that maximize civilian casualties. Criminals in Pakistan and other places are lending their drug trading networks to these terrorists. So that's why, in conclusion, we need to be imaginative, integrative, and improvising in our future. Thank you.

Remarks of Panelist Dr. Newton Howard, Director for the Center of Advanced Defense Studies, Washington, DC

> *One may ask why terrorists have not successfully debilitated our cyber infrastructure. The reason is because cyber infrastructure is used as part of a larger, controlled system.*

My talk addresses a critical part of the homeland security battle space. I will be introducing you to a cyberspace known as "service-oriented architecture." First I'll describe the architecture and then get into threats and vulnerabilities.

Service-oriented architecture is a unique, emerging type of integrating software. A lot of government and large industry organizations are adopting the architecture. It's a very natural transition because it treats software as a service and allows for flexibility that is essential in our current diverse software environment. In our systems, permission sharing is essential, and it's something that is common to the industry. If you define several areas of work very well and I allow for these areas to interact, then I am migrating toward a service-oriented architecture. A tremendous amount of existing legacy systems and open sources also forces the move toward service-oriented architecture. The transition to service-oriented architecture systems creates a very interesting threat space. That interesting threat space is being addressed by my research group. We are trying to understand and codify the most common method used in that space – Extended Markup Language.

We started out by looking at interoperability in permission sharing and the associated dilemmas posed to the law enforcement community. We came up with some interesting results looking at schemas that solved this problem. Then we noticed that we were opening up vulnerabilities that go back to the early 1990s. The firewalls that we have, secure routers and other protection measures may be circumvented in the transition to service-oriented architecture. We are opening this threat space again in our quest for better operating systems.

In upgrading software, the higher the level of abstraction, the more you are allowed to pass and process information seamlessly within a service-oriented architecture. Such loose coupling actually makes the use of this software architecture quite lucrative. I won't get into schema limitations, messaging types, and service methods. It is more useful to give you some examples of application problems.

In digital health and patient records, privacy issues are paramount. Problems also crop up in justice information sharing between national echelons, where protection of sensitive information and intelligence data are a concern. Here, the front-line echelons on the ground need sensitive information. The need to protect that information and make it available on the ground is a difficult challenge. In the telecommunication industry, the shift in use from actual voice services down to the other forms of services poses some interesting problems in the enterprise services software area. In business and government data centers such as Google and military command centers, you will see service portals aligned between agencies of certain departments and programs. So, service-oriented architecture is ubiquitous and has been in use for some time. It has been brought to the forefront because of its power and profitability.

In the computer world, one basically moves from the physical layer up the stack. As a result, we are noticing an attack pattern that focuses on the application layer, which is at the upper end. This presents a challenge in that something that which appears to be harmless network traffic may be actually passing malicious codes capable of disrupting infrastructure. A lethality issue relative to Service-Oriented Architecture where skills that are replicated over a very wide network, attacks may have multiple effects whose severity increases by virtue of their distributed nature. Such "swarm" attacks have serious implications regarding homeland security.

One may ask why terrorists have not successfully debilitated our cyber infrastructure. The reason is because the cyber infrastructure is used as part of a larger, controlled system. But if terrorists can find a way to develop a commander-controlled system in concert with a physical attack, then it is possible to increase lethality by improving the chances of a penetration attack. As a concrete example, if power grids or other utilities move into a service space for convenience including software control of parts of the service grid, then vulnerable portals will exist for physical attacks.

Gartner's group has predicted that 70 percent of vulnerabilities previously eliminated by Cisco and our firewalls will be reopened by the introduction of these services, which is true.

Service-oriented architectures exist and we had them for quite a long time. Their implementation has become more convenient with the advent of XML language because it's a portable and easy to learn.

The big question is, "How do we implement service-oriented architectures without increasing the risk?" Dynamic business interoperability is something that is really essential for the homeland security community to address. And we are seeing faster migration to these architectures because of the inherent efficiencies. Like all technological capabilities, it can be exploited to cause harm. Issues include federated identity, user identity verification, biometrics, privacy, swarm attack potential, and control of physical infrastructures through cyber gateways.

Gartner's group has predicted that 70 percent of vulnerabilities previously eliminated by Cisco and our firewalls will be reopened by the introduction of these services, which is true. We recently published a simple threat model that treats XML as the carrier of lethal payloads. Anyone who has a computer in here should be alert to the fact that within a few minutes of coming online, your computer became a target of multiple groups who are checking your personal information and surveying your system to identify your IP owner and content. Through well-known methods involving simple, apparently innocuous queries they can identify exploitable vulnerabilities in your system. They can then use old common messages for attack.

However, the biggest concern is the next generation attacks where users erroneously assume a certain level of security in their virtual private networks (VPNs). The user is absolutely certain that he has a secure tunnel, that no one else is in there where in fact a malicious organization is there waiting for you. As soon as the user enters the space, the malefactor learns how to penetrate.

The threat model that we have developed basically looks at payload/content threats. I would be delighted to share our research publications with you. X-Pass Injection is actually an interesting favorite of mine. Of course, buffer overflow was identified as a problem some years ago. However, this well-closed penetration is in fact something that is reopened along with DNS poisoning. In next generation attacks, we're concerned about backend targets subjected to multi-phase attacks. As previously mentioned, having these services distributed increases the effects/lethality of the attack in terms of bringing down the entire network. We are now codifying these threats – i.e. creating a harness where we actually simulate the attack and document the effects for the benefit of industry partners.

The necessary countermeasures that exist today for service-oriented architectures, including firewalls, are not in place. That is not a criticism of any industry partner, but Cisco and our other colleagues are not yet set up to do the necessary deep content inspection. The available validation techniques are not sufficient. Our computers are slow as it is processing the heavy content that we are deal with, let alone adding another layer of XML to inspect data containers, There is a growing "appliance business" to help us offload the security issues. This enables our computers to become portable and just deal with processing data rather than screening and preconditioning.

Solutions include hardening of applications and better coordination in the detection business. It will also be important to do a better job of publishing service-oriented architecture threats and vulnerabilities ahead of time. My group likes to work in the cognitive computing area and model things in natural settings. We find it useful to follow a model looking at human intent. Our model looks at a pattern of threat based on malicious intent and being aware of the associated internal and external factors. Our objective is to identify these threats earlier in the cycle - before we find our infrastructure totally softened and being prepped, if you will, for penetration. We think of our work as developing a cyber surveillance space.

Remarks of Panelist Dr. Noel Hendrickson, Professor of Philosophy, James Madison University

Here is a quiz. What is the first thing on every list concerning what to do in response to a crisis?

A. Don't panic.
B. Get on the first plane out of town.
C. Call a Philosopher.
D. Start out with a really bad joke.

> *Critical thinking skills are essential for everyone in the security community, whether they're in the military, whether they're in intelligence, whether they're in business, whether they're in law enforcement, whether they're in policy, or whether they're even citizens.*

The correct answer is, of course, A. Don't panic. Or at least that's what we tell everyone, don't panic. But let's think about that for a minute. When we tell people not to do something, it is never as useful as telling them what to do. What is it that we want people to do? Well obviously we want people to follow all of the well-reasoned plans that we have been talking about today. But, where do we get these plans? And more importantly, where do we get the capacity for people to understand and evaluate those plans and then implement them. Ultimately, this capacity comes from the ability to think critically. We need to learn to evaluate things not in terms of emotional responses, but rather terms of evidential support.

Any successful infrastructure security plan must be grounded in certain fundamental reasoning skills. Critical thinking skills are essential for everyone in the security community, whether they're in the military, whether they're in intelligence, whether they're in business, whether they're in law enforcement, whether they're in policy, or whether they're even citizens.

Unfortunately these skills are not innate. If anything, our innate thinking tendencies are the opposite of critical thinking. Critical thinking skills have to be taught. A major factor determining our future security will be our success at teaching reliable and relevant critical thinking skills. This will require us to develop a new model of critical thinking that is adequate to the task. In keeping with the theme of the panel, there are some important questions to consider to provoke thinking and vision for the future. These are questions that we are addressing as we develop a new information analyst curriculum at James Madison University.

Every major university offers courses in critical thinking. Unfortunately, the two extant models that we have in academia for teaching critical thinking are, arguably, inadequate to the task of addressing security needs. And as a result we have been working on a new model. But first let's look at what's wrong with the old models.

The best known model of critical thinking that's out there is what may be called the "generalist" or "positive mental habits" model. In this approach, critical thinking is primarily the acquisition and improvement of certain general rational procedures. This approach addresses critical thinking as a generalized skill set, i.e. rational self-awareness, fair-mindedness, clarity, carefulness and thoroughness. Now obviously these skills should be part of any critical thinking package. The strength of this approach is its high relevance. Its elements – clarity, thoroughness and so forth – can be applied to any problem or situation. Unfortunately, this approach has a weakness – low reliability. It's very difficult to formulate very precise rigorous standards for what the elements mean. This makes it very difficult to claim that you are teaching people how to do it – it's hard to measure and assess what you are doing.

The second model, which tends to be favored by my fellow philosophers what may be called the "Particularist" or "Informal Deductive Logic" Model. In this approach, critical thinking is the assessment of the soundness of deductive arguments. As you might guess, this approach has the exact opposite set of strengths and weaknesses. The strength of this approach is its high reliability. When you get a deductive argument and you can assess its soundness, it's pretty easy to learn how to get that right and assess how well people are doing it. On the downside, the approach is low in relevance. We don't get very far trying to deduce the intentions of terrorists that we have never met. Of course even if we have met them, we are going to have trouble trying to deduce what their intentions are.

As a result, there is a need for an essentially new model. Ultimately, the goal is to formulate a new approach that maximizes both relevance and reliability. The quest for a new critical thinking model is being addressed in conjunction with the development of a new Information Analyst curriculum at James Madison University.

The idea is to take the most powerful and important tools and concepts from the furthest, highest regions of the ivory tower, that have been ignored or dismissed at the working level because of their conceptual difficulty, and actually bring them down and show how they genuinely help solve real life problems. This can be done by explaining them in every-day terms and demonstrating their use in understandable applications. I contend that these concepts will prove quite useful. Given present time limits, the description of the approach will be brief. I would be happy to provide the longer version of this talk to anyone who is interested. The actual full implementation of teaching these concepts will span four semesters at JMU.

We face four defining challenges for reasoning in the security context. To address these challenges, there are four specialized applied reasoning methods or skill sets that we can use. These four skills sets will eventually constitute a baseline of core critical thinking skill packages that all of our future leaders will need whether they are in military, or intelligence, or law enforcement, or private business.

The first challenge is uncertainty. This is certainly an obvious one. We have to use information that is incomplete and imperfect most of the time. In response we need to talk about hypothesis testing – the ability to think critically despite having to use information that is limited in both relevance and reliability to infer the most plausible hypothesis. In this regard, we need to learn about "abductive inference" and "confirmation" theory.

The second challenge is irrelevancy. As we hear many times the problem isn't too little information, it's too much information, much of which may be irrelevant. How do we respond to that? What we need to do – and we have a second course for this – is focus on a causal analysis skill set. Typically when we talk about relevance what we are really interested in is what's actually affecting the outcomes of interest. We need to think in terms of how to distinguish correlations from real causes.

The third challenge is indeterminacy. Certainly in the intelligence context, we're interested in the intensions and future actions of other people and people have free will – there are lots of things they may do. We have to be able to handle the fact that there are many different outcomes of people's possible behavior. And in response we develop a counterfactual reasoning ability. The counterfactual reasoning skill set provides a framework for considering alternate possibilities and their consequences. It is all about answering the provocative, but really hard "what if" questions.

Fourth, we face the challenge of utility. We're not doing this analysis just for its own sake but to inform decisions about complicated and difficult dilemmas with tight time constraints. This necessitates the development of a strategy assessment skill set – the ability to think effectively about challenging choices by optimizing the utilities of all of the involved parts. This will include "gain theory," and "rational decision theory."

Each course that we are developing has to have a certain type of structure. We want two things: relevance and reliability. The imparted skill set must be applicable to real problems. And we need to be able to count on these methods as being genuinely trustworthy. It is necessary to bring together the two things that don't typically go together: the ivory tower and the real life. Because I'm a philosopher, I can complain about my fellow thinkers.

The courses will have the structure of the most advanced concepts, principles, and methods that are out there. In addition it will be important to continue to develop and expand the courses to be relevant to evolving real-life cases of interest. Half of these courses will be devoted to a practicum format: applying reasoning tools to a broad rang of real life cases. In our current pilot of the hypothesis testing course, we distinguished thirty different hypothesis testing strategies. But then, we demonstrate, depending upon what strategy is chosen, different outcomes are possible. For example, in dealing with questions such as, "Why do some terrorists choose to implement attacks using chemical weapons?" we find that the result depends on the hypothesis testing strategy selected.

The model that I am working on and endorsing is critical thinking as a rigorous application of hypothesis testing, causal analysis, counterfactual reasoning, and strategy assessment skill sets to real-life problems. The objective is to transfer these skills sets out of the academic community where people pursue them simply for their own sake. The skill sets exist – we need now to tap into them. It will be important to use every resource we have. Our success at this task will provide major benefits on the future horizons of infrastructure protection. Thank you.

Remarks of Panelist Mr. Frank J. Cilluffo, Associate Vice President for Homeland Security, George Washington University

The concept of critical thinking is extremely important. We need to think critically. There is an old inside-the-beltway tactic, especially used by many policy advisors: "When in doubt, sound pessimistic." We appear better informed and if dooms day does not occur we can always pat ourselves on the back and take credit for averting yet another disaster. There is another old saying that is apropos: "A pessimist is an optimist with experience." But we do have some optimism here in terms of how we can, should, and are looking at homeland security issues. The title of the symposium, "Engaging the Frontlines" is quite appropriate at this juncture. We are now translating plans into action, nouns into verbs in our current homeland security endeavors. We are not just engaging the frontlines, but enabling the frontlines. Quite honestly, everything we do should be focused on enhancing capacity closest to the frontlines in the war on terrorism, closest to those who are ultimately going to turn victims into survivors, closest to those that are ultimately going to be able to act.

We have a tendency too look through the world in the lens of the crisis de jour.

The biggest lesson from Katrina was the paralysis – the paralysis of analysis. The lesson here is the importance of pushing decision making closest to where situational awareness is most acute, closest to where the men and women in the fog of crisis who have the best information and have the ability to act. We can't wait and micro-manage decisions from Washington. It's the conundrum of how to cover the waterfront at the same time insuring local maneuverability and flexibility where it matters.

John Noftsinger was correct in his remarks – we have a tendency to look through the world in the lens of the crisis de jour. Often we march into the future backwards and fight yesterdays wars and that's understandable because, as Americans, when we see we did something wrong we want to do everything we can do to get it right the next time around. While it is important to strive to get things right, we should avoid being too reactive.

Shortly after 9/11 the fulcrum understandably swung heavily toward homeland security and counter terrorism issues and some of the prophylactic measures we need to protect Americans. Arguably some of the national disaster issues were not on that short priority list. At present, I think we are seeing the reverse. The pendulum is now right back to where we were five years ago due to looking at the world through the lens of yesterday's crisis. The way to get around this is to adopt the all hazards and preparedness planning, programs, policies, and procedures to address natural, accidental and malicious disasters.

Response measures will be similar for any type of wide scale disaster. Obviously there are going to be some new unique and boutique capacities and capabilities we need if we're responding to a biological warfare agent or pandemic influenza, hurricanes or earthquakes. We need to be able to look at this in a much more holistic way to maximize our limited resources and enhance our abilities to respond to any type of event. This is a bit of a challenge in terms of where the funding is coming from.

It is also important to look at where the threat is. We've got to look through the eyes of the adversary – a huge challenge within the intelligence community. We can't send men and women with blonde hair and blue eyes knocking on Bin Laden's cave saying, "hey we're here to join." We need to be able to have the cultural awareness, understanding, capacity, capability, and the ability to penetrate trusted familial networks. If you look at Al Qaeda itself, we have actually made a huge dent in the "Al Qaeda Classic." This is Osama bin Laden's organization in Swahili. Most of the leadership there has been incarcerated, killed or are clearly on the run.

But this doesn't mean terrorism has gone away. What we've seen is the morphing of Al Qaeda. It was never had a monolithic organization. Bin Laden appeared to act more like a Chief Financial Officer for a loosely affiliated network or networks. Now he has transitioned from the CFO to a Chief Spiritual Officer entirely. We are starting to see rifts in the Al Qaeda network, for example between Al Zarqawi and Bin Laden's organization. If you look at Al Qaeda today, it is franchised, like Kentucky Fried Chicken, Coca-Cola, and McDonald's. The franchised groups think globally but act locally. The glue that keeps them together is trust. That's the same glue that keeps us together to be able to improve our capacities to respond. We need to look at how we can lessen the trust among these organizations. The power struggle within Al Qaeda poses some real opportunities to divide the resulting factions.

A major question within the intelligence community after 9/11 was "What do we see next?" It's fair to say that since the Cold War, threat forecasting has made astrology look respectable. While we don't have a crystal ball, we know that Osama bin Laden's organization was clearly looking for the 9/11 plus attack. He needed credibility in the streets and the caves. But Al Zarqawi doesn't need a 9/11 plus attack to feel he's succeeding. Psychologically, numbers of smaller terrorist incidents could have a much greater effect and impact on Americans. Such attacks are the lower hanging fruits that we will have a very hard time detecting, discerning, deflecting, or disabling in advance. We may see lower consequence, but higher likelihood sorts of attacks in shopping malls or other public places. We are starting to see a bit of a change in the threat environment.

> *We are never going to be in a position where we can protect everything, everywhere, all the time from every perpetrator and attack. This approach would create a society in which we would be directly infrining upon what we are trying to preserve.*

I had the privilege and opportunity to be in the White House while we designed some of our homeland security strategies, policies, and programs. As the father of four young children, it was the sniper incident that had huge effect and impact in my own family notwithstanding the friends we lost on 9/11. But the sniper incident, not knowing who, what, where, when, the next shooting would occur had a huge psychological effect on us, especially in concerns about our children. This was effective terrorism, accomplishing the goals of eroding trust and undermining confidence in our government, our institutions, our values, our policies, and our officials.

We are looking at a new threat environment that poses some opportunities, but also some serious consequences. And we should always remember that this is a cat and mouse. It's not a game, but we've got a thinking predator that bases its actions on our actions. If we harden one target or defend against one modality of attack, they identify the new path of least resistance, strike another target, or find a new means to attack a conventional target. It is important that we be proactive, not looking backwards, and recognize that we are shaping the threat. This is not all bad. Ultimately we want to minimize and manage risks. We are never going to be in a position where we can protect everything, everywhere, all the time from every perpetrator and attack. This approach would create a society in which we would be directly infringing upon what we are trying to preserve. We need to be honest with ourselves as American people that we are going to have to assume risks. We cannot eliminate all risk.

On the bright side, this symposium and others like it are important in the quest to identifying and manage risks. We need cross discipline discussion of innovative approaches and technologies that improve our ability to reduce risks. If there is a silver bullet, it will result from discussions among leading edge experts in overlapping disciplines. Symposia such as these provide opportunities to look at things in new ways by tying together various disciplines. This is very exciting. The National Academy of Sciences, in particular, has recognized that and deserves kudos for their efforts to foster interdisciplinary approaches to such tough challenges.

There are some important intelligence issues that need to be addressed. Alternative analyses and the red-team thinking is so critical as we look ahead. There is a problem with "group think" that occurs when everyone is looking at a certain challenge from the same perspective or from a similar discipline. We need to always be questioning assumptions that all of us take to the policy planning table. This was the biggest challenge when we were putting together our homeland security initiatives. An inside joke was that the law enforcement representatives wanted to string people up and the intelligence community representatives wanted to string people along. The health community representatives just wanted to deal with the strung out. Each community had very different views of homeland security problems and solutions. And terms mean different things to different communities. Surveillance means something very different to the military, which was looking at it from a seafloor eye perspective, to law enforcement which was literally thinking about surveying a target. To the health community, surveillance means disease epidemiology. To the American people, surveillance is a rights issue. There are a number of challenges as we address intelligence as we seek to engage and enable the frontlines.

An important missing ingredient in the intelligence area is the ability to have the customer, in a consumer driven model, drive requirements. The customer should have a role in driving intelligence and information requirements. There are many at the state and local level and senior level who seem to think that someone in Washington is behind a green door with all the answers; that they have all the required intelligence. When we kick down that door, it reveals an incomplete puzzle. We have pieces. But there are many challenges. There is a signal to noise challenge. We often have too much data that may or may not contain the data we need. And most of the data we do have is perishable – it's useless 24 hours later if relative to indication-warning capacity.

We've done a disservice to the American people in explaining the role of intelligence. Intelligence is the lifeblood for the campaign of the war on terrorism. The first objective should always be to get there before the bomb goes off; not react heroically after it does. But we need to be able to parse out indication and warning from everything else intelligence does to support operations including military, law enforcement, and diplomatic.

We have never done warning well. The Holy Grail is to know when and where an attack will happen. This is not a risk communication challenge. If we know when and where a bomb will detonate, the event will be preempted. Rarely do we have the when and where data… it's looking for the needle in the hay stack. We've got to go through what the military went through for about eight years and go through the Goldwater-Nichols equivalent of unifying our homeland efforts on the federal, state, and local level and ultimately including the American people. We also need to go through the Goldwater-Nichols process in terms of information and intelligence sharing.

I close with a quote from my favorite philosopher, New York Yankee great Yoggie Bera, who once said, "The future aint what it used to be." Each one here has a responsibility and a capability to shape that future in a way that enables a more secure life for ourselves and our next generations.

Future Horizons Panel Summary

Dr. Ciluffo made an interesting point about answers lying at discipline edges, at boundary overlaps/intersections among disciplines and organizations. We've endeavored to organize this conference with this in mind. We also recognize that answers don't reside in one university. We are pleased to have several regional universities participating in this symposium.

Question from audience: My name is Lou Pearlman with HSPI. I have a question for Noel Hendrickson. I'm intrigued by your list of four defining challenges for reasoning in the security context. I am wondering if your list is complete. There's another challenge that you may or may not have considered. I was trained originally as a mathematician, while my functional skills rested to dust a long time ago there are a few concepts that stuck with me. One of them, which I discovered early in my academic career, was the concept of the well formed problem. Mathematicians figured out a long time ago that they were a lot better at thinking up problems than they were at solving them. Along the lines somebody got the idea that maybe a lot of these problems don't have solutions and that's why we are spending our whole lives trying to solve them. So they developed an actual test to determine at the beginning whether a problem has any solution to avoid wasting time trying to solve it. Subsequently, I spent the next three decades working on policy and strategy problems in both public and private sector. My experience is that the vast majority of my clients don't know about ill-posed problems. In fact many of the problems that come up, not just Homeland Security, you could pick any field, may not have solutions. Particularly in the political realm, problems are often defined in ways that really have no solution. So I think that somewhere in your Architecture of Critical Thinking there should be an element which screens the formation of problems to ask "Is this a real problem? Can it ever be solved?" That would be very helpful. Have you included this?

Response from Noel Hendrickson: Thanks for that question. Essentially I've structured my approach to respond to what is already out there in the academic community. I am rebelling against the generalist model where one tries to be clear and aware of any assumptions or the typical logical model where one focuses on one problem type. Essentially I've done the taxonomy in terms of different types of problems and so for each of those problem types one of the first things that we have to do is learn how to recognize those which are genuinely solvable problems in each of those types. So that would be something that is essential in each of my four challenges. The way that I set up the taxonomy is partially to distinguish this approach from the others. Your point is absolutely right.

Question from audience: I had a question that came up earlier in the day but it seems to be a potential question for each of the panels. Perhaps this panel can answer it. Earlier today someone mentioned that 85 percent of the infrastructure is owned by the private sector. In trying to figure out how to understand and protect these systems, we go to the owner/operators and ask, "What are your most critical assets? If it's not critical then we won't include it in our assessment." This is the common way we simplify the problem. As a local government person, when we looked at our critical infrastructure in areas that dealt with our county's 911 system and associated government services, our local exchange carrier would say, "That system is not critical to our business as a local exchange carrier, so I won't put that on my top list of priority critical infrastructure." As a result, what is a critical system for the protection of local lives and property may not be on the discussion list in the first place. There needs to be a way to not only look at who owns the critical infrastructure, but get the perspective of the customers actually using the systems. This makes our job a little more complicated.

Response from Frank Cilluffo: This is a well-founded question. One of our biggest gaps today is building the business case for Homeland Security. An important related question is what exactly is the public/private partnership? I suggest that there are some tools and instruments that haven't been leveraged here. How far does the market place take security? And how much beyond the market place solution needs to be done? How much is enough? The difference between where we are to where we need to be needs to be described. And we must also identify the incentives and/or regulations or disincentives needed to get us where we need to be. I espouse the "mitigate before litigate/regulate" philosophy. We don't want the trial lawyers driving security over the experts. State and local governments have not spoken as one voice to the private sector. They need a common voice from a supply chain management perspective. One other sector that has not been tapped is the insurance sector. In the quest for behavior change, the government, historically, can only go so far. The insurance sector has had a much greater success rate in changing behavior. Prior to the great Chicago fires, all we had were fire brigades. We responded to the ensuing fire prevention codes that resulted. In the case of seat belts, it wasn't Uncle Sam that drove that process; rather it was the insurance sector. There is much room for some innovative thinking in this arena.

Introduction

Dr. John Noftsinger, Jr., James Madison University

Thanks again to the panel. As you've noticed the theme of our conference has been "Engaging the Frontlines." One of our objectives is to start a conversation with our university, industry and government partners. Our final keynote speaker is a person that bridges these three sectors. John McCarthy is Executive Director of the Critical Infrastructure Protection Project at George Mason University. Many of you don't know that John also had a long career in government. He worked in the White House on Y2K remediation and later in the Critical Infrastructure Assurance Office. He also had a distinguished 20 year career in the Coast Guard where he worked in operations as a first responder and ship captain. He has also worked in industry. John is to be commended for his leadership of the CIPP project. The project was established by U.S. Congressman Wolf who suggested that the effort involve collaboration between George Mason University and James Madison University. John has made it work and through his leadership skills and commitment to the partnership John has always been a fair player and an advocate for our partnership. It's my pleasure to introduce John McCarthy.

> *Technology is our front as the enabling element across every sector, public and private. Instead of moving at the speed of a train or at the speed of a plane or at the speed of a ship, we are moving at the speed of electrons and microchips. This has accelerated the lag between the technology advance and policy development.*

Keynote Speaker

John McCarthy, Director and Principal Investigator, Critical Infrastructure Protection Project, George Mason University

Multi-institutional, multidisciplinary, support the national agenda – those were the three watch words or watch phrases that we set between George Mason University and James Madison University when we put the Critical Infrastructure Protection Program together. Congressman Frank Wolf from Virginia was visionary. He said many months before 9/11 that we needed to have a multi-institutional, multidisciplinary approach to the emerging field of Critical Infrastructure Assurance.   His ideas included addressing both public and private perspectives and how the marketplace influences the agenda. The CIP program has incorporated these ideas into our program.

Today's agenda has done a great job of addressing the three watch words.   I would like to acknowledge our executive sponsor within the federal government. The National Institute of Standards and Technology has been an exceptional partner, especially in view of the political pressures associated with homeland security related efforts. NIST has been very gracious in the way that they have overseen the series of significant grants associated with the CIP Program. We at GMU and JMU appreciate that very much.

Public/private partnership is extremely important and I greatly appreciate the question that just came up concerning state and local government interaction with the private sector. It has been a core theme of the CIP Program from the very beginning. The CIP Program is located within the GMU Law School. This brings a very conservative market-oriented economic view to the effort. I appreciate Frank Cilluffo's ability to put very complex concepts into quick and simple terms. The role of the market and the private sector is important given that a large majority of our critical infrastructure is owned and/or operated by the private sector. You've heard the statistic, and it is true. But what are the real implications of this? Where are we?

The 1997 seminal work of the President's Commission on Critical Infrastructure and Protection was the first complete document jointly developed by the government and the private sector to look at emerging threats to our infrastructures in the post cold world. Technology, policy and the law elements are all driving together. Technology is out front as the enabling element across every sector, public and private. Instead of moving at the speed of a train or at the speed of a plane or the speed of a ship, we are moving at the speed of electrons and microchips. This has accelerated the lag between the technology advance and policy development. And law is behind policy. The technology/law gap is very wide. We're seeing this play out in the front pages of our newspapers today.

What are the implications of this lag? What should we do to close the gap? Frank Ciluffo made a reference to going down the road where we lock down requirements on our private sector and the public sectors that serve them. This implies imposing regulations and hard-core standards to enhance security. This approach begs the question, "What kind of society does this engender?" The answer can't be put into the sound bite. Extensive dialog among stakeholders will be required to get to a solution.

The 1997 PCCIP Report started the dialog. And we are still talking about the many of same, difficult issues. We are still trying foster better information sharing. We all agree we need better information sharing between the public and private sectors. But what are the requirements to get better information sharing?

We have learned a lot of lessons from 9/11 and Katrina. I would argue that Y2K provided a kind of a dress rehearsal for a national CIPP event. The TWA 800 event taught us many lessons. It involved the Coast Guard, the FBI, and the National Transportation Safety Board under the National Response Plan, which was the controlling document at the time. The CEO of TWA, and his designate on scene were integral to the command decision-making process. This is an important case study in public-private partnership.

There are many good models of coordinated public/private response and reconstitution processes. Hurricane Katrina has uncovered new issues that need to be addressed for extremely wide-scale disasters. The National Response Plan is simply not robust enough to deal with the complexity and the scale and scope of the super-regional events that we will face in the future. Katrina showed us that the private sector has enormous capability and robustness in terms a supply chain and securing that supply chain. It's their business. The question becomes how to integrate that capacity into not just what the federal, state, and local government response elements are doing but also what the other sectors are doing. This makes for a very difficult problem due to complexity.

Under the CIP Program, we serve as an executive agent for DHS to support the government-industry sector coordination process. There are industry sector coordinating councils which are formal bodies representing the 17 critical infrastructures. Each of the critical industries has a government sector coordinator. Private sector perspectives vary from sector to sector. There are the "Cement Sectors" – the old fashioned bridges, locks and dams which are very engineer-oriented. Their systems are fixed geographically. The locations of nuclear plants are well-known… they appear on every map. For these facilities, there is a close, regulatory relationship between the public and private sectors. There is a requirement for a National Asset Database. Since we don't yet have a National Asset Database, we don't have a good public/private dialogue. The nuclear industry representatives don't care to be in a new national database because they are already on the map. There are a fixed number of facilities and those facilities already have communication with the government. In the case of water facilities, we get a similar reaction.

With respect to the banking and finance community, representatives question the "fixed facility" model. They maintain that their sector is better viewed as a set of large scale processes that may or may not involve fixed facilities. How does the check clearance process work? It's really five processes within five super banks around the world. Although the full system is not an individual facility, fixed facilities house pieces of the process. The challenge is to isolate process sub-elements within a database. It becomes a tough physical question.

In the case of individual retailers, let's take a sports example. Pick the management of Yankee Stadium, or any stadium in the country. Indicate that they are to be included in the National Asset Database. As with any public facility, they will start to come up with questions. The questions might be, "If my facility is in this database so that the state and local and national government agencies know that I'm in the National Asset Database, what liability do I have? If I have an anthrax incident at Yankee Stadium, does being in the National Asset Database require me to have extra security? And, if I don't have that security will I be held liable?" This raises enormous questions for the private sector and they often respectfully try to avoid National Asset Database status.

There is a major report on the public/private partnership called Neglected Defense: Mobilizing the Private Sector for Support of Homeland Security by the Council on Foreign Relations, authored by Steve Flynn, a very bright, former Coast Guard officer. One of his key issues is the National Asset Database and the fact that we don't know what our critical infrastructures are. Part of the problem is that the private sector doesn't want you to know what the critical infrastructure is. They have complex reasons that go beyond the obvious. In dealing across infrastructure sectors, it's not possible to develop a monolithic approach.

Another important issue is identifying trusted people. In our response to Katrina and other catastrophic events, the individual industry sectors actually have very, very good communication networks across what are very disparate, competitive groups. In preparing for Y2K, one group I worked very closely with was the anti-virus community within the cyber and the microchip industry. The Internet community in itself fiercely opposes regulation. The internet is designed not to be regulated.

On the other hand, there is a strong network of informal network management that takes place every single minute. Apandemic of internet attacks take place every single day. This pandemic is being managed globally by informal trusted networks. Most of those informal trusted networks are based on informal relationships among trusted people. Many of these people operate unnoticed and may sit behind a console at a data center. They may have a card in their back pocket that tells them who to call for coordination in the event of different types of incidents.

A key challenge between the public and private partnership in the prevention and response world in the next five years is how to formalize those trusted individual networks. How do you formalize this to a degree that it can then become a trusted process into a national response system? This is a huge challenge. A major sea change in thinking concerning industry operation and information sharing is required.
There are also major challenges concerning how the government will protect that process once it is in place.

We need to get away from preparing for the last event. An all-hazards approach is important. We must focus on the core capabilities needed from the human, policy, doctrinal, and technical perspectives. What are the core capabilities we need to assemble and execute quickly including the right group of public, private, and academic experts for the next disaster that will address the catastrophe as it evolves? As the incident begins to scale up, we must be able to rapidly connect with the right people.

An interesting case study is the business round table, the top one hundred companies in the world. At the CEO level, these companies have the ability to pick up the phone and get a majority of the top CEOs on the line on short order. To teleconference every senior leader among government agencies is not as easy. The Department of Defense is an exception. But the private sector has, at high levels, the capability to do that. That's where the government-industry partnership needs to be – trusted individuals, trusted processes so information can be shared with protection and safeguards. I estimate that we are four or five years away from having a true trusted exchange of information. It's not that we don't have the technology. There are personal biases that get in the way.

We keep looking for the quick fix and answer. The 80 percent fraction of critical infrastructure owned and operated by the private sector that creates an additional 80 percent complexity that we've never dealt with in the national and homeland security arena before. The government has always been able to deal with this problem by sending in the Marines or the Navy or the Coast Guard. Now we find with homeland security, and critical infrastructure in particular, that we can't simply send in the uniformed services to deal with problems. Different solutions are needed. Yet, we haven't totally retooled on the public side to be able to accommodate private sector response.

How do we take advantage of private sector ad-hoc initiatives that are very good response mechanisms? We saw many good examples during the response to Hurricane Katrina. Heroic response from Wal-Mart and Fed-Ex are outstanding examples. These companies and others like them have the ability to reach and get to their people and their processes in rapid fashion. During a disaster how can we marry public and private efforts into the required, accountable response process?

Accountability and responsibility are very important in disaster response. In the end somebody had to stand up and take responsibility. After Katrina, it was Mr. Brown. We can't forget the fact that government is about accountability. We must be able to hold the person in charge of a process to a level of accountability.

Question from audience: I am Brian Shakoda from Cubic Corporation. Dealing with the private sector in the past, particularly when you are talking at these conferences or where you are attending, quite often I found out that principals are unwilling to acknowledge possible threats or vulnerabilities because such admissions may make them liable unless they implement countermeasures. Is that still prevalent in your experience?

Response from John McCarthy: That, in my opinion, is a strong argument for making a business case for countermeasures. Once a company admits being part of a critical infrastructure, what responsibilities attach to that? This a key question. It's easy to say lets all jump on the critical infrastructure band wagon to support the national strategy. But reality sets in, and when you start to pull the threads on the sweater the company's General Council stands up and taps the CEO on the back and says, "Why don't you sit down and be quiet; let's not go down that road of volunteering that information yet."

Q&A for the Day and Closing Remarks

Dean Jerry Benson, Dean of the College of Integrated Science and Technology, James Madison University

I would echo that we have had the opportunity today to engage in discussion and hear from some very learned persons about the diversity of the issues facing us in the quest for national preparedness. As I thought through what I heard today, messages seemed to fall in two categories: partners, and roles and responsibilities. Beginning with President

Rose's remarks this morning, universities can play a major role in engaging the front lines. We often think in terms of a three legged stool with universities, government sectors, and private sectors working together. Based on what I have heard today, I would add a fourth leg to that stool: professional organizations. These would include the National Academies, our co-sponsors, the Federal Facilities Council, speakers from ASME and other professional groups that are taking these issues very seriously and stepping forward to participate in the conversation.

We have heard a lot today about complexity. I am somewhat conflicted about that. We certainly know that our infrastructures are interdependent comprising a "system of systems." The challenge is to foster communication among the infrastructure sectors and among the government jurisdictions that would be affected by multiple infrastructure failures. John McCarthy, John Cilluffo and others have talked about the importance of communication and the coordination across the different sectors and incentives, both economic and humanitarian, to make this happen. It is also clear that better understanding of cascading failures, including the ability to model interdependencies will be critical.

We have heard a lot today about the need to better communicate and educate the public about homeland security contingencies and preparedness. There is a conflict between the complexity of what we are dealing with and trying to make it so simple that we can actually convey it. I often think of Edward Tufte's admonishment concerning "death by Power Point" or the illogic of Power Point. If we try to reduce everything to three bullet points, we really do lose the complexities that we are dealing with.

Finally, concerning responsibilities, a strong unifying message from today's presentations was that the local level and individual preparedness are all-important. Dutch Thomas talked about the oxymoron of national preparedness at the local level, but that is really what is needed: establishing and sustaining a consistent thread of continuity from the national strategy to the State and local levels.

I will end my remarks by again harkening back to President Rose's comments and the basic mission of our institution: to produce educated citizens. A major theme of today's proceedings is citizenship and the responsibilities of each and every one of us. In closing, I was thinking earlier today that after all we have heard today, everything from electromagnetic pulses and the different bioterrorist threats. Thanks to Greg Saatoff, who coined the new term we learned today, we can all go home and "planic."

Prof. Steve Knickrehm, James Madison University

Dr. Benson and I have been given the challenging task of picking some common themes and messages from what we have heard today. The task is somewhat daunting due to the great wealth and diversity of perspectives represented on today's panels both from the standpoint of research interests and career backgrounds.

Our theme for today was "Engaging the Frontlines." Our unstated assumption in organizing this symposium was that our national focus on national level solutions cannot work by itself. That was born out today as we heard it again and again from the speakers that all disasters are local. For me the unifying theme of today's work was that we need to take personal responsibility, exercised locally by communities. That is the direction in which we need to be moving in the future within homeland security and disaster preparedness and response endeavors. I see three strategies emerging concerning how we can get people to take personal responsibility exercised locally within their communities. The first is to communicate. People need to know their responsibilities. We have got to move beyond the mind set the Federal Government will come in on the white horse and make everything okay in the first two hours. That is not true and we have been told that it is not true. The second strategy is empowerment. Citizens need to know that they can take responsibility. The third strategy is education. Citizens need to be aware of threats and hazards and how to prepare and respond as they take action at the local level.

My thanks to each of you, speakers and audience members, for making this event happen, and for your roles on the front lines as we leave. On behalf of James Madison University, The National Research Council, and the Federal Facilities Council, we really appreciate all of you being here today.

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

Daniel Caprio,
The Progress & Freedom Foundation

Robert Cofod
BankDetect

Grant Cooley
Predicate Logic

Al Costantine
Science Applications International Corporation

Raghu Dev
Paladion

Gene Garlick
Northrop Grumman Information Technology

Matthew Keller
Corsec Security, Inc.

Michael King
Northrop Grumman Information Technology

David Ladd
Microsoft Corporation

Jacqueline Liggins
Ingenium Corporation

Richard Little
University of Southern California, School of Policy, Planning, and Development

William Maconachy
National Security Agency

Sadaat Malik
Cisco Systems, Inc.

Louis McDonald
Virginia's Center for Innovative Technology

Jeffrey Payne
Cigital, Inc.

Brendan Peter
LexisNexis Special Services, Inc.

Ben Plowman
Luna Innovations

John Rice
United States Navy

Kyndra Rotunda
Shook, Hardy & Bacon

Fenton "Dutch" Thomas
MSA Incorporated

Jay Willer
Consultant to Natural Gas Industry

Lee Zeichner
Zeichner Risk Analytics, LLC

Host Contact Numbers

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;
email: lstanley@nas.edu

James Madison University

Dr. John B. Noftsinger, Jr.

Associate Vice President of Academic Affairs
for Research and Public Service
MSC 4107, Harrisonburg, VA 22807
Phone: 540-568-2700; Fax: 540-568-1784;
email: noftsijb@jmu.edu
www.jmu.edu/research

Mary Lou Bourne

Director, Office of Technology Transfer
MSC 4107, Harrisonburg, VA 22807
Phone: 540-568-2865; bourneml@jmu.edu
www.jmu.edu/ott

Dr. George H. Baker

Associate Director for Infrastructure Research
Institute for Infrastructure and Information
Assurance
MSC 4102, Harrisonburg, VA 22807
Phone: 540-568-8767; bakergh@jmu.edu

Taz Daughtrey

Associate Director for Software Development
Institute for Infrastructure and Information
Assurance
MSC 4103, Harrisonburg, VA 22807
Phone: 540-568-2778; daughtht@jmu.edu

Cheryl J. Elliott

Assistant Director for Marketing and External
Relations
Institute for Infrastructure and Information
Assurance
MSC 4111, Harrisonburg, VA 22807
Phone: 540-568-4442; elliotcj@jmu.edu

Kenneth F. Newbold, Jr.

Associate Director for Finance and
Administration
Institute for Infrastructure and Information
Assurance
MSC 4111, Harrisonburg, VA 22807
Phone: 540-568-1739; newbolkf@jmu.edu

Dr. Ruben Prieto-Diaz

Associate Director for Information Assurance
Institute for Infrastructure and Information
Assurance
MSC 4103, Harrisonburg, VA 22807
Phone: 540-568-1665; prietorx@jmu.edu

Featured Speakers

Daniel W. Caprio, Jr., The Progress & Freedom Foundation, Senior Fellow and Executive Vice President

Prior to joining the Foundation, Mr. Caprio served as Acting Assistant Secretary for Technology Policy and Chief Privacy Officer for the Department of Commerce. While at the Department of Commerce, he oversaw all Departmental activities related to the development and implementation of federal privacy laws, policies, and practices.

He served as Co-Chairman of the Federal Radio Frequency Identification (RFID) Council and Chairman of the Department of Commerce RFID Working Group. Prior to working at the Department of Commerce, Caprio served for six years as Chief of Staff to Federal Trade Commissioner Orson Swindle, where he worked as principal technology policy advisor with specific emphasis on information security, privacy, and global electronic commerce. In December 2001, Mr. Caprio was appointed to the United States Government Experts Group to revise the Organization for Economic Cooperation and Development (OECD) Guidelines for the Security of Information Systems and Networks. Caprio has held a range of staff positions in the U.S. Congress and state government. Mr. Caprio's initial tenure at the U.S. Department of Commerce was during the Reagan Administration, where he directed Congressional Relations for the Economic Development Administration.

In addition to his public sector experience, Mr. Caprio worked in corporate government relations at KPMG, a global financial and accounting firm. He received his B.S. in Political Science from James Madison University.

William R. Graham, Ph.D., Science Advisor to President Reagan

Dr. Bill Graham has over forty years of experience in areas such as national telecommunications, nuclear survivability, threat analysis, ballistic missile defense, counter- proliferation, and government technology development.

Dr. Graham chairs the U.S. Title XIV Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. Appointed to this position by the Secretary of Defense, Dr. Graham is leading the review of the nature and magnitude of potential high-altitude EMP threats to U.S. civilian and military assets and systems.
Dr. Graham also serves as a member of the Defense Science Board (DSB). The DSB members are designated by the Undersecretary of Defense (ATL) to advise the Defense Secretary and JCS on technical, scientific, manufacturing, and acquisition matters of special interest to the Department of Defense. Other commissions that Dr. Graham has served on include the congressionally mandated Commission to Assess United States National Security Space Management and Organization, which was chaired by Mr. Rumsfeld. He also served as Commissioner of the Commission on the Ballistic Missile Threat to the United States from 1997 to 1998. From 1986 to 1989, Dr. Graham was the Science Advisor to President Reagan. Concurrently he served, under Senate confirmation, as the Director of the Office of Science and Technology Policy in the Executive Office of the President. He also chaired the Federal Coordinating Committee on Science, Technology, and Engineering, which provides high level coordination of federal research and development programs. This placed him as the President's Executive Agent with State of Emergency powers to assume control of U.S. telecommunications assets. To maintain preparedness, he chaired the Joint Telecommunications Resources Board, a government and industry coordinating body established to assist him in the execution of his State of Emergency responsibilities.

Dr. Graham graduated the California Institute of Technology with BS in Physics. He earned his MS in Engineering Science at Stanford University, as well as his Ph.D. in Electrical Engineering. His honors include Membership in Tau Beta Pi and Sigma Xi Honor Societies, as well as receipt of the Air Force Commendation Medal and the Defense Special Weapons Agency's Lifetime Achievement Award.

Michael Lowder, FEMA Acting Director of Response

Mr. Lowder serves as the Acting Director of the Response Division for the Federal Emergency Management Agency (FEMA) in Washington, D.C. A member of the Senior Executive Service, Mr. Lowder is responsible for coordinating the development and execution of interagency plans, policies, and procedures and for response operations in Presidential disaster and emergency declarations and other Incidents of National Significance. Mr. Lowder has been designated and served as a Principal Federal Official (PFO).

Prior to this, Mr. Lowder has held the Deputy Director and Director of Operations positions in the Response Division as well as the Response and Recovery Division Director for FEMA's Region IX, headquartered in San Francisco, California. In that capacity, he was responsible for delivery and coordination of all disaster planning, response, and recovery activities in the region, which include the States of Arizona, Nevada, California, Hawaii, as well as the US Territories of Guam, Commonwealth of the Northern Mariana's, American Samoa, the Republic of the Marshal Islands, and Micronesia.

Mr. Lowder has been a member of FEMA's National Emergency Response Team (ERT-N) and the Domestic Emergency Response Team (DEST), and has worked on numerous disaster operations throughout the United States.

Prior to his work with FEMA, Mr. Lowder has over 25 years of experience in the law enforcement and emergency services field in the State of North Carolina. Mr. Lowder served for a number of years as a Special Agent with the North Carolina State Bureau of Investigation. Following that, Mr. Lowder was the Director of Emergency Services with Bladen County, North Carolina.

Mr. Lowder has represented FEMA at conferences in Russia, Australia, Japan, the UK, Taiwan, and Turkey, as well as throughout the United States. Most recently, he represented the U.S. at a NATO-RUSSIA counter terrorism exercise in Kaliningrad, Russia. He has served on numerous national committees, including NFPA's Forest and Rural Fire Protection Committee.

John A. McCarthy, George Mason University, Director and Principal Investigator, Critical Infrastructure Protection Project

John A. McCarthy has a unique blend of executive level government, business, and academic experience in the areas of national security relative to the maritime and transportation sectors as well as in-depth knowledge of the governmental interagency process. An experienced program and crisis manager, he has been particularly successful in delivering policy and technical solutions that are time sensitive and national/international in scope. Mr. McCarthy is a recognized thought leader within the information security policy and risk management arenas and is considered an authority on critical infrastructure protection and business continuity management issues by industry and government practitioners alike.

With more than 20 years as a commissioned officer in the United States Coast Guard, Mr. McCarthy served in a wide variety of demanding field command and senior staff positions including command-at-sea and personal Aide to 19th Commandant.

Mr. McCarthy holds a B.A. degree in Psychology from The Citadel--Military College of South Carolina, Charleston, S.C., and an M.S. in Information Resource Management (specialization in government) from Syracuse University, Syracuse, N.Y. He is also a graduate of the National Defense University--Information Resource Management College, Washington, D.C., and the U.S. Naval War College--Command and Staff College, Newport, R.I. Additionally, he is a distinguished graduate of the Department of Defense Chief Information Officer Certificate program. His military and civilian awards include the Legion of Merit, the Meritorious Service Medal (three awards), the Combat Action Ribbon, and the Vice President's National Partnership for Reinventing Government "Hammer" Award.

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

Dr. Linwood H. Rose, the fifth president in James Madison University's 95-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.

Dr. Rose was recently appointed to the National Infrastructure Advisory Committee (NIAC) by President George W. Bush. The committee makes recommendations regarding the security of the cyber and information systems of the United States. Dr. Rose has served as the chair of the Virginia Council of Presidents. He also has recently served as commissioner, Virginia state chairman, committee chair and chair of the executive council of the Southern Association of Colleges and Schools (SACS); and as a member of the James Madison Commemorative Commission of the U.S. Congress.

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 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. Dr. Rose served as acting president in the fall of 1997, and was chosen as JMU's chief executive in September 1998.

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 degree in educational administration and supervision from the University of Tennessee, and his doctorate in higher education administration from the University of Virginia.

Panelists

Prevention Panel

Mr. Fenton "Dutch" Thomas, MSA Incorporated (Panel Moderator) – National Preparedness

Dutch Thomas has twenty-five years professional and management experience overseeing complex operations involving a wide range of participants. At present, Mr. Thomas is the Manager for National Preparedness Program for MSA, Inc. Under his guidance the process of emergency preparedness was initiated and is currently ongoing at the Army National Guard Readiness Center. It is the model of choice for the best, most efficient training of people in facilities potentially targeted for terrorist attack. The focus is on the person working in the facility, not merely the structure itself. Included in the area covered by the emergency preparedness plan is the neighborhood surrounding the site and its interface with the surrounding community. The efficacy of this approach was verified in the aftermath of Hurricane Isabell when Readiness Center staff gave credit to their emergency preparedness training in assisting their families in coping with the effects of the storm. This is the prototype for what is to become a nationwide effort.

Dutch is a highly regarded professional officer with career focus on working with diverse groups in the areas of Support to Civil Authorities, Crisis Management and Emergency Coordination and joint operations. During his military service in Washington he coordinated Military Support to Civil Authority for all declared disasters and designated National Security Special Events from August 1992 till March 2002 while serving in the Directorate Of Military Support (DOMS), as Chief of Military Support for the National Guard while at the National Guard Bureau, and while serving as the Department of Defense Military Support Liaison Officer to the Federal Emergency Management Agency. Team builder and project organizer experience in the operations of State National Guard agencies and the National Guard Bureau. Mr. Thomas is intimately familiar with the mobilization process of the Reserve Components, especially the National Guard, and knows full-well the impact mobilization has on Guardsmen and their families.

Mr. Taz Daughtrey, James Madison University, IIIA Associate Director for Software Development – Cyber Security and Risk Assessment

Taz Daughtrey is Associate Director for Software Development in James Madison University's Institute for Infrastructure and Information Assurance. He has been a member of the JMU Computer Science Department for the past five years, after a lengthy career in industry. A Fellow of the American Society for Quality, Taz was the Founding Editor of the Society's peer-reviewed journal SOFTWARE QUALITY PROFESSIONAL. He has taught and consulted on a wide range of software assurance and management topics throughout North America, Europe, and Japan.

Mr. Richard Little, University of Southern California, Director, Keston Institute for Infrastructure – Critical Infrastructure Protection

Richard G. Little is Director of the Board on Infrastructure and the Constructed Environment of the National Research Council (NRC) where he develops and directs a program of studies in building and infrastructure research and maintains outreach and liaison with federal agencies, the legislative branch, and affiliated organizations. He has directed NRC study activities, participated in workshops and panels, and written several papers dealing with blast-effects mitigation and critical infrastructure protection. Mr. Little served as the Study Director for the 1995 NRC report, Protecting Buildings from Bomb Damage and the 2001 report, Protecting People and Buildings from Terrorism: Technology Transfer for Blast-effects Mitigation, and a just-completed review of the Interagency Security Committee (ISC) Security Criteria.

Mr. Little has more than thirty years experience in planning, management, and policy development relating to public facilities, including fifteen years with local government. He has been certified by examination by the American Institute of Certified Planners and is a member of the Federal Planning Division of the American Planning Association. Mr. Little holds a B.S. in Geology and an M.S. in Urban-Environmental Studies, both from Rensselaer Polytechnic Institute.

Mr. David Moore, National Security Agency – Cognitive Solutions

DAVID T. MOORE is a career senior intelligence analyst and technical director at the National Security Agency. He also teaches at the Joint Military Intelligence College, Washington, DC; is an adjunct faculty member of the National Cryptologic School; and has taught at Trinity University, Washington DC. He holds a Master of Science of Strategic Intelligence from the Joint Military Intelligence College. He is the author of CRITICAL THINKING AND INTELLIGENCE ANALYSIS, (forthcoming, Joint Military Intelligence College Press, May 2006); co-author of "Intelligence Analysis, Does NSA have What it Takes," Cryptologic Quarterly, 20, nos. 1/2 (Summer/Fall 2001); "Core Competencies for Intelligence Analysis at the National Security Agency," in Bringing Intelligence About: Practitioners Reflect on Best Practices, Russell Swenson, ed (2004); "Evaluating Intelligence: A Competency-Based Approach," in the International Journal of Intelligence and Counter Intelligence, 19, no. 2 (Summer 2005); and author of "Species of Competencies for Intelligence Analysis," Defense Intelligence Journal, 11, no. 2 (Summer 2002). Over two decades of intelligence assignments, both in the Washington DC area and abroad have provided Mr. Moore expertise in the areas of intelligence analysis competencies, methods, and standards including years of advocacy for, and mentoring of, best practices in intelligence.

Dr. Peter Pham, James Madison University, Director of the Nelson Institute for International and Public Affairs – Diplomatic Solutions

Dr. J. Peter Pham is Director of the William R. Nelson Institute for International and Public Affairs, an assistant professor of justice studies at James Madison University, an affiliate faculty member of the Department of Political Science, and an associate faculty member of the Africana Studies Program. Dr. Pham also holds an appointment as Resident Fellow at JMU's Institute for Infrastructure and Information Assurance (IIIA).

Dr. Pham received his B.A. in economics from the University of Chicago and his doctorate in political and social ethics from the Gregorian University in Rome, Italy. Among other academic qualifications, he holds graduate degrees in international affairs, administrative law, and international law, as well as theology and canon law. His research interest is the intersection of international relations, international law, political theory, and ethics, with particular concentrations on implications for United States foreign policy and African states as well as religion and global politics. During the current academic year, he is directing a pilot study on Africa's place in a strategic vision of America's future energy security.

Dr. Pham is the author of over one hundred essays and reviews on a wide variety of subjects in scholarly and opinion journals on both sides of the Atlantic and the author, editor, or translator of over a dozen books. Dr. Pham is the recipient of a 2005-2006 Academic Fellowship on Terrorism from the Foundation for the Defense of Democracies and is presently completing a study on terrorism in Sub-Saharan Africa.

Prior to coming to James Madison University, Dr. Pham served as an international diplomat in Liberia, Sierra Leone, and Guinea from 2001 through 2002, and has been recently appointed to serve as an official U.S. delegate on the election observation mission to monitor the Liberian national elections in October 2005.

Protection Panel

Mr. Patrick Bridge, Virginia Department of Health (Panel Moderator) – Regional Emergency Preparedness and Response

Dr. George Baker, James Madison University and IIIA Associate Director for Infrastructure Research – Infrastructure Assessment

Dr. Baker was instrumental in organizing JMU's Institute for Infrastructure and Information Assurance (IIIA) and now serves as Associate Director for Infrastructure Research. he Served as JMU's principal investigator on the National Capital Region Infrastructure Assessment Program. He recently participated on the Congressional EMP Commission. Baker is former director (1996-1999) of the Defense Threat Reduction Agency's Springfield Research Facility, a national center for critical system vulnerability assessments. Much of his career was spent at the Defense Nuclear Agency (DNA) leading national programs in nuclear protection, underground testing and standards development. He is a member of the NDIA Homeland Security Executive Board, the National Research Council Infrastructure Roundtable, the Institute of Electrical and Electronic Engineers, the Directed Energy Professional Society (Charter Member), and the Association of Old Crows. He is an EMP Fellow and holds a Ph.D. from the U.S. Air Force Institute of Technology.

Dr. Jerry Brashear, American Society of Mechanical Engineers – Protection Standards

Jerry Brashear has had more than 30 years' experience in evaluation, planning and risk management. Currently, he is a Program Director for the Innovative Technologies Institute, LLC, a wholly owned, non-profit subsidiary of the American Society of Mechanical Engineers (ASME), where he serves on the senior management team developing and implementing Risk Analysis and Management for Critical Asset Protection (RAMCAP), a national, sector-by sector program, and is leading a team designing a program in regional risk management and resilience. Previously, he directed the University Consortium for Infrastructure Protection in his capacity as Associate Director for National Capital Region Projects of the Critical Infrastructure Protection Program (CIPP), George Mason University School of Law. From 2001 to 2004, Dr. Brashear founded and directed the Center for Petroleum Asset Risk Management at The University of Texas, an integrated, interdisciplinary (geology, petroleum engineering, and business) research and development program. Since 1996, he has also been the Managing Director of The Brashear Group LLC (TBG), an independent management consultancy that advises senior management of private firms and ministries on planning, policy, economic analysis and all-hazards risk management. For more than 20 years prior to founding TBG, Dr. Brashear served ICF Consulting and its predecessor, Lewin and Associates, Inc., as Senior Vice President, Director of the Oil and Gas Practice, and Member both of the Board of Directors of ICF Resources, the energy unit, and of the Management Committee of ICF Consulting, the parent firm. His education includes an AB magna cum laude, Princeton; an MBA, Harvard; and a PhD in Urban and Regional Planning, The University of Michigan.

Dr. Ronald Raab, James Madison University – Vaccine Development

Dr. Ronald W. Raab is currently an Associate Professor for the College of Integrated Science and Technology at James Madison University. Prior to his work at JMU, Dr. Raab worked at the University of California, Berkeley as an instructor. During his time at the university he developed and taught a course in DNA Recombinant Technology for non-science majors. Dr. Raab earned his Ph.D. Texas A&M University Molecular Biology/Genetics in 1988. Over the years Dr. Raab has been involved with many publications and has affiliated himself with many activities. Dr. Raab is the Faculty Advisor for the student chapter of the Virginia Biotechnology Association, in 1996 he served as Co-Chair of the Biotechnology and Engineering Committee for the Tri-Valley Economic Project, and he has also worked with the USAMRIID project.

Dr. Eric Tollar, SAIC, Senior Analyst for Radiological and Nuclear Countermeasures – System Analysis and Protection

Dr. Tollar is presently a senior analyst in the CBRNE Effects and Analysis Division at Science Applications International Corporation (SAIC). He is lead technical analyst for SAIC in the DHS Radiological and Nuclear Countermeasure Architecture Analysis Program, as well as lead risk analyst for Critical Infrastructure. Prior to this, he was the Vice President of Engineering at NIKSUN, Inc., responsible for the software and hardware development of the network monitoring product line. At Telcordia Technologies, Dr. Tollar was division manager of Data Warehousing Development, and director of the Professional Services Risk Analysis Department, specializing in risk analysis for telecommunications networks. Dr. Tollar graduated from Purdue University with a B.S. in Computer Science. He received his Ph.D. in Statistics from Purdue University.

Response Panel

Mr. Grant Cooley, Predicate Logic (Panel Moderator) – Secure Software

Mr. Cooley, a United States Navy veteran, has responsibility for Predicate Logic's east coast business development. Mr. Cooley has over 20 years of communications engineering experience as well as Navy and Joint Communication Systems development including all levels, implementation, and system integration and testing. Additional expertise includes development and operational testing of numerous communication systems, including SHF, EHF, UHF, HF, LF and VLF submarine communications equipment. Mr. Cooley retired after 20 years of naval service in the submarine community serving in the enlisted and officer ranks. Immediately prior to his retirement in 1998, Mr. Cooley was the COMSUBLANT Force C4I officer. Mr. Cooley has been with Predicate Logic since October of 1998 and was previously the Vice President of Global Network and IT Services. Mr. Cooley resides in Virginia

Beach, VA.

Mr. Joshua Barnes, MSA Incorporated – Continuity of Operations
A graduate of James Madison University with a B.S. in Geographic Science, Joshua has been engaged in preparedness related research for the past two years. His initial work with IIIA yielded several publications and both national and international-level presentations. Currently as a member of the COOP Program Team at MSA, Inc. he continues his research through Federal-level COOP support and community-based preparedness initiatives.

Dr. Lennie Echterling, James Madison University – Disaster Psychology
Lennis G. Echterling, Ph.D. is a Professor of Psychology at James Madison University, where he serves as Director of Counseling Psychology. He received his doctorate in clinical psychology from Purdue University and has more than 30 years of experience in crisis and disaster work. Following the 9/11 attacks, he worked as a Red Cross volunteer with survivors at the Pentagon. More recently, he provided disaster intervention services in Mississippi and Texas following Hurricanes Katrina and Rita. His books include "Crisis Intervention: Promoting Resilience and Resolution in Troubled Times" and "Ideas and Tools for Brief Counseling," both of which are published by Prentice Hall, and "Thriving! A Manual for Students in the Helping Professions," which is published by Houghton Mifflin. Dr. Echterling has received James Madison University's Distinguished Faculty Award, Virginia Counselors Association's Humanitarian and Caring Person Award, and the national Counseling Vision and Innovation Award from the Association for Counselor Education and Supervision.

Dr. Mark Kirk, University of Virginia – Emergency Medicine and Situational Management
Dr. Kirk is an Assistant Professor of Emergency Medicine for the University of Virginia. His clinical and research interests are in medical toxicology and acute poisoning, respectively. Dr. Kirk earned his M.D. in 1985 from the University of Kentucky College of Medicine. His residency was emergency medicine at Methodist Hospital and Medical Toxicology at Rocky Mountain Poison and Drug Center was his fellowship. He currently works mostly with acute and workplace poisonings.

Dr. Greg Saathoff, University of Virginia – Community Shielding
Dr. Saathoff is the Associate Professor of Research at The University of Virginia School of Medicine and has served as the Executive Director of the Critical Incident Analysis Group or CIAG since 1997. In 1995, he served as Psychiatric Consultant to King Faisal Specialists Hospital, Riyadh, Saudi Arabia. Dr. Saathoff became a Conflict Resolution Specialist for the FBI's Critical Incident Response Group in 1996. He is a consultant to the Virginia Department of Corrections and the Virginia State Police. As a member of CSMHI's faculty, he participated in the Estonia, Kuwait, and Georgia projects.

Dr. Saathoff is chairman of the Committee on International Relations of the Group for the Advancement of Psychiatry and has published papers on post-traumatic stress disorder, traumatic cultural effects, borderline personality disorder, biologic psychiatry and police psychiatry. Saathoff is currently a consultant to the Virginia Department of Corrections and the Virginia State Police.

Future Horizons Panel

Dr. John Noftsinger, James Madison University, AVP Research & Public Service and Executive Director, IIIA (Panel Moderator) – Partnerships
Dr. John B. Noftsinger, Jr. is the Associate Vice President of Academic Affairs for Research and Program Innovation, Executive Director of the Institute for Infrastructure and Information Assurance, and Associate Professor of Integrated Science and Technology and Education at James Madison University. Since 1998, his primary responsibilities include: facilitating external grant and contract funding, Homeland Security research programs, economic development, intellectual property and technology transfer, and academic public relations and service programs for JMU. He specializes in interdisciplinary program and grant development for the university. In 2002, Dr. Noftsinger was named by Governor Warner and was reappointed by Governor Kaine as Co-Chair of the Virginia Research and Technology Advisory Committee, which he has served on since its inception in 1999. He has spearheaded the successful development, funding, and implementation of the following programs at JMU: Institute for Infrastructure and Information Assurance, Mine Action Information Center, Shenandoah Valley Technology Council, Virginia's Manufacturing Innovation Center, Workforce Information Network (WIN), Civil War Institute, Valley of Virginia Partnership for Education, William R. Nelson Institute for Public Affairs, the Critical Infrastructure Protection Program and the Shenandoah Valley Business Gateway.

A native of Roanoke, Virginia, he is a 1985 cum laude graduate of James Madison University with a double major in Political Science and Public Administration and a minor in Business Administration. He received his Master of Arts degree in Higher Education Administration from The Ohio State University in 1987. In 1997, he received his doctoral degree in the Higher Education Program at the University of Virginia Prior to his tenure at JMU, Dr. Noftsinger held student services positions at Frostburg State University in Maryland from 1987-89 and at The Ohio State University from 1985-87. He came to JMU in 1989 as Director of Continuing Education and External Programs and Administrator of the Valley of Virginia Consortium for Higher Education. He was appointed Deputy Secretary of Education for the Commonwealth of Virginia in 1993-94 and returned to JMU in 1994 as Assistant Vice President for Academic Affairs. Dr. Noftsinger has presented at numerous local, regional, and national events and conferences and has published significantly in the area of education/community partnerships, economic development, technology policy, higher education, and strategic leadership, including co-authoring a forthcoming textbook entitled Understanding Homeland Security: Policy, Perspectives, and Paradoxes to be published by Palgrave-MacMillan and co-editing a book entitled Leveraging Resources Through Partnerships, published by Jossey-Bass.

Mr. Frank J. Cilluffo, The George Washington University, Associate Vice President for Homeland Security and Director, Homeland Security Policy Institute – Policy Solutions

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. 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. Cilluffo joined GW from 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, Cilluffo 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, Cilluffo was responsible for engaging and building partnerships with the private sector, academic, and state and local officials and emergency responders on 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, Cilluffo spent eight years in senior policy positions with the Center for Strategic & 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, and information warfare and information assurance. Mr. Cilluffo has to published extensively in academic, law, business, and policy journals, and magazines and newspapers worldwide and has testified before the United States Congress on a number of occasions. Cilluffo 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.

Dr. Noel Hendrickson, James Madison University – Critical Thinking Skills for the Intelligence Community

Noel Hendrickson earned a Ph.D. in Philosophy from the University of Wisconsin in 2002. He currently teaches at James Madison University, where he is also piloting the C.A.S.E.S. Program (Core Analytic Skills Enhancement System)- a series of new specialized applied reasoning courses created to constitute the "Critical Thinking" component of JMU's developing Information Analysis Major. He is also working on a new model for evaluating alternate scenarios and their consequences (funded by IIIA).

Dr. Newton Howard, The Center for Advanced Defense Studies, Founder and Chairman -- Digital Defense

Professor Howard holds a Doctoral degree in Cognitive Informatics from La Sorbonne, France. Internationally he is a leading researcher on the Physics of Cognition (PoC) and its applications to Defense and International Security.

He is a graduate of the Faculty of Mathematical Sciences at the University of Oxford. His graduate work proposed the Theory of Intention Awareness (IA). Dr. Howard is the Founder and Director of the Institute for Mathematical Complexity and Cognition (MC2). Dealing with subjects related to cognition, complexity, and intentions, the work of this institute has implications for systems engineering and international security. He also heads the Descartes Institute for Mathematical Methods in Behavioral Codification and Global Security, focusing on behavior models and codification to develop new approaches for counter-terrorism based on in-depth analysis.

Dr. Howard advises several organizations in the US special operations community and has extensive experience of working in the industry. He holds multiple U.S. patents, and is the author of several publications in the areas of military information science, computer systems theory, and strategic thinking. He affiliated with US Intelligence Community and served honorably in U.S. Armed Forces as Strategic Intelligence Officer.

Featured Research

Africa and U.S. Security Interests

Dr. Peter Pham (phamjp@jmu.edu)
Africa's rapidly increasing capacity to supply global hydrocarbon needs as well as its potential for terrorist penetration and its geographically strategic location relative to both the Middle East and Europe make it imperative that the continent receive the attention it deserves from U.S. policymakers as the national security priority that it has already become.

As a first phase in a multi-staged undertaking, this project entailed on-site research as well exploratory conversations with African political leaders and scholars with an eye to developing future possibilities for collaborative engagements in policy research and education, training, and public awareness. It has subsequently been the object of ongoing interest on the part of both the U.S. Congress and agencies of the Executive Branch.
Poster @: www.jmu.edu/iiia/webdocs/17 Africa & Security interests.pdf

Biomanufacturing Group @ JMU

Dr. Ron Raab (raabrw@jmu.edu)
Dr. Robert McKown (mckownrl@jmu.edu)
The biomanufacturing group at JMU has established capabilities for cloning and expressing foreign genes in microbial systems, pilot-scale fermentation, protein purification and analytical testing of biological molecules. The laboratory offers small-scale production of recombinant proteins for research and development on a contractual basis as well as basic and applied collaborative research projects.
Poster @: www.jmu.edu/iiia/webdocs/8 Bioman Group.pdf

Bioterrorism: Defense through Knowledge

Jeffrey Muller (jmuller@predicate.com) with
Dr. Barbara Kreutzer, Advisor (kreutzbb@jmu.edu)
The threat of bioterrorism is real. The weapon has no boundaries. The enemy does. However, with the proper knowledge, we can stop the terrorist from their campaign of fear. Bioterrorism: Defense Through Knowledge is a multimedia educational resource about bioterrorism, delivered to the target audience through the web medium. The website provides an easy access to information about bioterrorism threats and the defense against these threats.
Poster @: www.jmu.edu/iiia/webdocs/1 Bioterrorism Website.pdf

Center for Energy and Environmental Sustainability

Dr. Christopher Bachmann (bachmacg@jmu.edu) and
Dr. CJ Brodrick (brodricj@jmu.edu)
The four cornerstones of the Center for Energy and Environmental Sustainability (CEES) include the air quality, water quality, alternative fuel, and renewable energy education and research programs within ISAT. CEES formalizes relationships that already exist within these groups thereby accomplishing multiple goals: Coordinate CEES-relevant work of students and faculty; Promote the unique energy and environmental capabilities and resources within ISAT and JMU; Enhance external relations, job placement, graduate student opportunities, and recruiting; and Expand existing external relationships and networks.
Poster @: www.jmu.edu/iiia/webdocs/10 Energy2.pdf

Container Tracking System

Dr. Helmut Kraenzle (kraenzhx@jmu.edu)
The Geographic Information System for Simulating Container Movement (GISSCM) is a prototype application to simulate a digital visual interface tracking system for the worldwide movement of containers and their contents with destinations to the United States.
Poster @: www.jmu.edu/iiia/webdocs/16 Containers.pdf

FALCON: Integrated Decision Support System for Chemical Incidents and Medical Preparedness

Dr. Michael Deaton (deatonml@jmu.edu)
FALCON is a concept design and prototype software implementation of an integrated, GIS-based decision support system for emergency prevention and management of hazardous incidents. Integrated elements include a medical response knowledge base, medical readiness assessment, a chemical plant security assessment tool, and geo-referenced regional chemical inventory data, health facility data and population data.
Poster @: www.jmu.edu/iiia/webdocs/14 FALCON.pdf

Financial Model to Estimate Internet Security Breaches

Dr. Faramarz Damanpour (damanpfx@jmu.edu)
International business and commerce has been experiencing dramatic changes via economic integration and globalization. Internet has played a key role in the way companies do business, and synergism has been created between Internet technology and global business operations. This study intended to shed light on the significance and interrelationship between business and technology, the existing barriers and security concerns, and to develop a model to estimate the cost of Internet security breaches.
Poster @: www.jmu.edu/iiia/webdocs/4 Financial Model.pdf

Humans as Critical Infrastructure

Josh Barnes
Holistic community-based preparedness is securing the Human Infrastructure, a process of establishing a community's preparedness baseline, facilitating positive

interactions among all community leaders i.e. leadership, faith-based leaders, emergency managers, medical providers, local business, economic developers, etc., and taking action to foster individual and community resiliency.
Poster @: www.jmu.edu/iiia/webdocs/2 Humans as CI.pdf

Indoor Air Quality Sensing and Alert/Alarm System

Dr. W. Gene Tucker (tuckerwg@jmu.edu) and
Dr. David J. Lawrence (lawrendj@jmu.edu)
We are investigating the feasibility of a detection and alarm system using sensors that detect heat released or absorbed when airborne pollutants react with specific surfaces. We are modifying a very sensitive thermopile temperature sensor developed in-house by applying chemical or biological coatings to the sensor that will react with air pollutants of concern.
Poster @: www.jmu.edu/iiia/webdocs/6 air sensors.pdf

Info Sec Education

Dr. Hossain Heydari (heydarmh@jmu.edu)
www.infosec.jmu.edu
People involved in information security must be able to understand and systematically employ and manage InfoSec concepts, principles, methods, techniques, practices and procedures drawn from U.S. statutes, current or pending. InfoSec experts must also understand procedures followed by the Department of Defense, federal, state and local governments, industry and businesses.

The JMU Master of Science in Computer Science with a concentration in Information Security program is entirely Internet-based, with courses designed so that students and professors can maximize use of their time asynchronously.
Poster @: www.jmu.edu/iiia/webdocs/11 Info Sec.pdf

Multi-dimensional Evaluation of Vocal Deception

Dr. Michael Hall (hallmd@jmu.edu) and
Dr. Chris Watts (wattscr@jmu.edu)
The development of alternative, voice-based technologies for the detection of deception.
Poster @: www.jmu.edu/iiia/webdocs/13 Vocal Deception.pdf

NSRAM Network Security Risk Assessment Model

Concept Development: Dr. George Baker (bakergh@jmu.edu)
Licensing: Mary Lou Bourne (bourneml@jmu.edu)
Marketing/Research Partners: Cheryl Elliott (elliotcj@jmu.edu)
Software Development: Taz Daughtrey (daughtht@jmu.edu) and Phil Riley (rileypb@jmu.edu)
NSRAM (Network Security Risk Assessment Model) is a tool for determining the probability of failure and repair/recovery time of complex systems comprised of a network or system of networks. The invention simulates a system of interconnected physical and cyber networks (such as electrical grids, communication lines, or waterways) as a representative model of the networks.
Poster @: www.jmu.edu/iiia/webdocs/12 NSRAM.pdf

Public Service Assessments

Dr. George Baker (bakergh@jmu.edu)
IIIA will use an integrated team of faculty and consultants with expertise in these areas:

- Threat Application and Environments
- Specific Operations and Support Systems
- Risk and Vulnerability Analysis
- Protective Measures and Systems

In order to better serve our clients, IIIA will:

- Investigate the entire system, breadth and depth.
- Identify common and unique site problems – lessons learned.
- Make practical recommendations for improvements.

Integration of lessons-learned into training packages.
Project deliverables will be conducted and distributed on a fee-for-service basis.
Poster @: www.jmu.edu/iiia/webdocs/19 Public Assessments.pdf

Quantifying Trustworthiness in System Compositions

Dr. Ruben Prieto-Diaz (prietorx@jmu.edu)
This research proposes a framework for quantifying trustworthi- ness in IT systems. To date, trust in IT systems is not well defined, and is usually regarded as a qualitative measure. Trust- worthiness in software is considered especially difficult to quantify.
Poster @: www.jmu.edu/iiia/webdocs/3 Trustworthy Systems.pdf

Radio Frequency Identification (RFID)

Dr. Geoffrey Egekwu (egekwuog@jmu.edu)
The development and application of Radio Frequency Identification (RFID) tags and readers are widely tested in inventory and supply chain management applications, but experts believe that as the technologies continue to improve, it could form the core of networks that will handle many activities, from monitoring the structural integrity of bridges to reminding you that the tub of coleslaw in the fridge is past its due date.
Poster @: www.jmu.edu/iiia/webdocs/9 RFID.pdf

Secure Software Development

Dr. Sam Redwine (redwinst@jmu.edu)
Secure Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software Version 1.0 is a document surveys the field in approximately 180 pages and provides educators, trainers, and others possessing knowledge of software but not of security a guide by topic to relevant, high-quality references containing more in-depth knowledge. JMU's Sam Redwine serves as Editor.
Poster @: www.jmu.edu/iiia/webdocs/15 Secure Software.pdf

Security of Small Community Water Systems

Kyle Tom with Dr. Thomas Benzing (benzintr@jmu.edu)

A local small municipality manages its own water supply and wastewater treatment systems. Our goal was to analyze the security of their water infrastructure to learn more about the challenges faced by small communities, specifically throughout the Shenandoah Valley. We used global positioning systems and geographic information systems (GIS) to create maps of the water systems throughout the town. In the GIS, we established a geometric network to analyze flow through the sewer system and identify areas that may be at risk. We described these risks and the many side benefits of a functional water infrastructure GIS for the town utilities manager and the rural community.
Poster @: www.jmu.edu/iiia/webdocs/5 Water Systems.pdf

Student Terrorism Studies

Dr. J. Peter Pham (phamjp@jmu.edu)

Undergraduate students at James Madison University have had exposure to issues of terrorism and political violence through the upper-level Seminar on International Terrorism course in the Department of Political Science which was introduced long before such course offerings became fashionable at many American universities and colleges after 9/11.

However, with Dr. J. Peter Pham, Director of the Nelson Institute for International and Public Affairs and Resident Fellow at the Institute for Infrastructure and Information Assurance, who currently teaches the course, the opportunities for JMU students to study both the challenges of the terrorist phenomenon and counterterrorism strategies have taken on a new dimension.
Poster @: www.jmu.edu/iiia/webdocs/18 terrorism studies.pdf

Vaccine Development

Dr. Ron Raab (raabrw@jmu.edu)
Dr. Robert McKown (mckownrl@jmu.edu)
Dr. George Coffman (coffmagl@jmu.edu)

To clone, express and purify various proteins for characterization and study as possible vaccine and diagnostic reagent candidates for USAMRIID.
Poster @: www.jmu.edu/iiia/webdocs/7 Vaccine Development.pdf

PROCEEDINGS

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 masters, 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.

JAMES MADISON UNIVERSITY®