SEPTEMBER 2003 / VOLUME 2, NUMBER 3

THE CIP REPORT

CIP PROJECT STAFF

John McCarthy, *Executive Director*

Emily Frye, *Associate Director, Law and Economics Programs*

Kevin "Kip" Thomas, *Associate Director, Research Programs / Research Associate Professor*

Rebecca Luria, *CIP Project Administrator / Executive Assistant*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

George Baker, *Associate Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click here.

Message from John McCarthy, Director, CIP Project

This issue of *The CIP Report* highlights the National Capital Region Project and GMU's contribution to the efforts of the District of Columbia, Virginia, and Maryland in protecting the region's critical infrastructure as well as the academic partnerships that will carry out the work involved. The National Capital Region (NCR) is unique - in addition to two states and the District of Columbia, it includes three branches of federal government, comprising the headquarters of almost every federal agency, 17 local governments, 35 law enforcement bodies, 2,100 non-profit organizations, myriad private sector interests and over 4 million Americans. The challenges to combating terrorism and protecting critical infrastructure in the NCR are significant and complex. I am pleased that George Mason University will play a role in meeting those challenges through its support of the Urban Area Security Strategy for the NCR.

The Urban Area Security Strategy provides a strategic direction for enhancing regional capability and capacity to prevent and reduce vulnerability of the NCR from terrorist attacks. Eight "Commitments to Action" were identified and have shaped the goals and objectives for NCR terrorism and response planning. Virginia's State Chair has responsibility for the coordination of the Critical Infrastructure Protection Commitment to Action. GMU will report to the State Chair and has partnered with other academic institutions with key capabilities to carry out this role.

The concept for this effort was developed over the last four months under the direction of the NCR Steering Committee, comprised of the Deputy Mayor of D.C. and the governors of Virginia and Maryland. Under the direction of Michael Byrne, the first Director for the Office of National Capital Region Coordination at the Department of Homeland Security, GMU is preparing for these new responsibilities.

THE TECH CENTER
National Center for Technology & Law
CRITICAL INFRASTRUCTURE PROTECTION PROJECT

In addition, I recently had the honor of appearing before the Joint Homeland Security Subcommittee (Subcommittee on Cybersecurity, Science and Research & Development, and the Subcommittee on Infrastructure and Border Security) to discuss the implications of the Northeast Blackout on CIP. You will find my testimony in this month's newsletter. As part of my discussion, I noted the requirement to accelerate analysis on mapping and identifying vulnerabilities and interdependencies, which directly correlates to the objectives of the Critical Infrastructure Protection Commitment to Action.

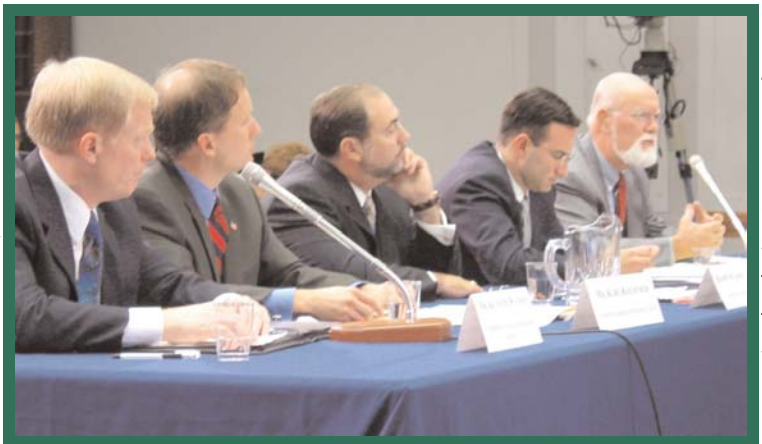
We are excited to take part in this challenging and important effort under the NCR Project and have assembled a diverse and accomplished set of partner universities, including James Madison University, Virginia Polytechnic Institute and State University (VA Tech), the University of Virginia, Howard University, the University of Maryland, Norfolk State, and Old Dominion University. We look forward to the work ahead.

Testimony of John A. McCarthy
Director of the Critical Infrastructure Protection Project, George Mason School of Law

Before a joint hearing of the House Subcommittee on Infrastructure Security and the House Subcommittee on Cybersecurity, Science, and Research & Development
September 4, 2003

Thank you, Mr. Chairman and distinguished members of the Committees for the honor of appearing before you today. I am here to testify about issues and challenges in providing for critical infrastructure protection in the context of the recent blackout and how George Mason University is assisting in this agenda.

As a preliminary matter, I'd like to introduce the Critical Infrastructure Protection (CIP) Project, within the George Mason University School of Law, where I serve as Executive Director. The CIP Project has a unique role in building an inter-disciplinary research program that fully integrates the disciplines of law, policy, and technology. We are developing practical solutions for enhancing the security of cyber networks, physical structures, and economic processes underlying our nation's critical infrastructures. The CIP Project is specifically charged with supporting research that informs needs and requirements outlined in the various National Homeland Security Strategy documents. Since its inception a little over a year ago, we have sponsored more than 70 substantive research projects, touching leading scholars at 20 universities - with James Madison University as a leading partner - and focusing more than 200 graduate and undergraduate students on security related studies. CIP Project sponsored research ranges from highly technical efforts to design new security protocols for cyber systems, to mapping the vulnerabilities of various infrastructures, to exploring the legal and business governance implications of information sharing, to experimental economic analysis of the energy sector under the direction of Dr. Vernon Smith - the most recent Nobel Laureate in economics.



John McCarthy (center) and the panel of speakers

In addition, GMU leads an academic consortium of regional scholars, supporting CIP vulnerability analysis and interdependency identification for homeland security planning efforts here in the National Capital Region. We are working closely with the Department of Homeland Security to ensure vulnerability assessment and modeling tools are developed locally that can be deployed nationally.

The Northeast Blackout provides a clear example of disruption to our vital infrastructures. I will focus my comments today on those issues I believe are key areas of critical infrastructure protection that require continued emphasis. These are:

- The need to develop a comprehensive understanding of infrastructure vulnerabilities and tools to assess these vulnerabilities;
- The need to better understand the complex interdependencies between infrastructure sectors; and
- The need to develop effective systems of public-private partnerships that afford true information sharing.

The Blackout and its consequences serve as an effective yardstick by which to measure critical infrastructure protection development since 9/11. On a positive note, most areas that were affected by the blackout had power restored within 24 hours. Considering the large

(Continued, Page 3)

McCarthy Testimony *(Cont. from Page 2)* geographic area, the number of jurisdictions involved, and the international aspects of the Blackout, this was a sound response. Particularly noteworthy were the cross-sector public private communications that took place away from the eyes of the media. These communications involved industry, state, local and national decision-makers. I believe these relationships were not ad-hoc responses to the Blackout, but the result of the efforts of the past decade in developing a means for enhanced information exchange between the public-private sectors.

First, the Blackout experience highlights our nation's serious problems with infrastructure, including poor comprehension of our vulnerabilities and lack of awareness or preparedness for the interdependencies of infrastructures. The Blackout stresses the need to further identify, map and define our critical assets and properly assess their vulnerabilities - as have 9/11, the first bombing at the World Trade Center, Y2K, and numerous debilitating cyber attacks. Comprehensive infrastructure mapping allows us to assess exactly where vulnerabilities are, what redundancies are needed, and how to recover quickly from a disruption by physical or cyber means. It is important to map out each of the critical infrastructures, how they work with each other, and study the possible effects that the loss of one infrastructure will have on others. This type of network and vulnerability mapping is vital in addressing and managing future infrastructure disruptions. In addition, this will afford the insurance and reinsurance industries the opportunity to gather sufficient information so they can determine their appropriate role in the terrorism risk insurance arena.

Congressmen Mac Thornberry and Dave Camp, Subcommittee Chairs

These analyses must also include evaluation of myriad possible scenarios that may pose threats to critical systems and provide identification of physical and process actions, as well as economic incentives to industry that afford greater resiliency and security of key infrastructure assets. For example, in the short term, the use of redundant electrical generation at hospitals in New York City resulted in virtually no loss in service delivery capability for emergency responders and health care providers during the Blackout.

Next, the Blackout also highlights infrastructure interdependencies, which underscore the need to develop a comprehensive understanding of how these infrastructures work together. The loss of power to the energy grid implicated more than just our energy infrastructure; it cascaded into several other infrastructures. For instance, sewage piled up at a Harlem treatment plant because there was no power to pump it through the facility. A diver had to be sent in through 40 feet of liquid sewage in order to get the pumps working again. GMU, as well as other research universities, have particular technical expertise to bring to bear in both the risk assessment of our critical assets and the advanced understanding of infrastructure interdependencies. We are fully supporting DHS's efforts to accelerate understanding in these key areas.

Finally, the interconnectivity of modern infrastructures goes beyond the technical systems themselves. The human element of critical infrastructure protection is equally, if not more important. People must communicate in order to prevent and respond to critical infrastructure failures. This high-level communication process is complex and involves many layers of connectivity. It is perhaps the most vital piece of effective infrastructure protection we can provide because we cannot anticipate every contingency. Robust information sharing must afford sufficient levels of detail at both the executive and operational levels. It should candidly identify vulnerabilities, prioritize key infrastructure assets, and allow public and private officials to prevent, respond to, and recover from potential disruptions. By the same *(Continued, Page 13)*

Urban Area Security Initiative for the National Capital Region: GMU to Lead CIP Commitment to Action

In recognition of the importance of securing our nation's urban areas, the Bush Administration partnered with Congress to provide substantial federal resources to selected urban areas across the country, including the National Capital Region (NCR). The Urban Area Security Initiative (UASI) Grant Program is designed to enhance the ability of first responders and public safety officials to secure the area's critical infrastructure and respond to potential acts of terrorism. The Program's intent is to create a sustainable national model program whereby urban areas can share the lessons learned and best practices with other urban areas around the nation.

In July 2003, communities within the NCR completed an assessment that led to the development of the Urban Area Security Strategy for the National Capital Region. In addition to the inputs from the assessment, the National Strategy for Homeland Security, the Eight Commitments to Action for the NCR, and the State Template published by the Homeland Security Council also contributed to the creation of the Strategy.

The UASI Eight Commitments to Action are focused through four key areas: planning, training, exercise, and equipment. George Mason University's role in Critical Infrastructure Protection Oversight falls under planning. With collaboration from university, industry, and government partners, GMU will conduct an analysis of each critical infrastructure sector. The analysis will center on assessing vulnerabilities.

There are a wide range of deliverables that this project will generate in the context of the NCR Project as depicted in the table below.

In addition to the specific actions proposed for the Critical Infrastructure Protection Commitment to Action, GMU is in the process of coordinating its efforts with the Training and Exercise Commitment to Action to ensure that those vulnerabilities that are identified, the assessment practices uncovered, and the business practices and policy implications revealed can be tested to allow an ongoing evolving process of enhancing security over time.

The overall intent of this effort is to use the National Capital Region project as a real world laboratory exercise to evaluate and propose future methods of critical infrastructure protection activities. ❖

Project Deliverables for CIP Commitment to Action
Conduct an assessment of the previous infrastructure vulnerability assessments data: Detailed "range and depth" analysis of previous assessments by government, industry, and other sources
Gather data: Detailed collection of the data identified in Deliverable One
Capture best practice processes: Evaluation of assessment data analysis to develop best practice auditing tools
Build a process or framework for future infrastructure vulnerability assessments: Development of a process or series of processes that allow for reliable, comparable, auditable, and accountable assessment over time
Develop best business practices and policy issues / recommendations: Development of policy recommendations and business practice procedures that afford dissemination and adoption of infrastructure specific standard methods of vulnerability assessments
Based on analysis performed and process frameworks developed, perform an assessment to determine and define appropriate response and mitigation actions from the perspectives of local, state, federal and industry sectors

NCR Project and Models of Collaborative Information Sharing

Ami C. Carpenter
Institute for Conflict Analysis and Resolution


Ami Carpenter

George Mason University has identified a number of key activities within the Critical Infrastructure Protection Commitment to Action of the National Capital Region (NCR) Project. First, is a coordinated effort spearheaded by a team of leading academics to develop a flexible data model that will be used to assess regional vulnerability.

The second goal of the NCR project is to build relationships between industry representatives that will use the flexible data model once it has been researched and developed. The hope of NCR architects is that collaborative relationships will be facilitated by engaging industry leaders in the shared process of research and development of the vulnerability assessment tool. Here, it will be important to know what practices best facilitate information sharing.

The Information Sharing Team has responsibility for developing this framework for collaborative information sharing. To do so, it will gather data in similar fashion to the indexing of previous vulnerability assessment actions that allow us to identify best assessment practices. The team will catalog best information sharing practices utilized by the many invested persons and institutions working with vulnerability assessment data. In addition to secondary resources, such as literature reviews, there are ongoing collaborative processes within the NCR project that provide a rich source of data for investigating how collaboration has
(Continued, Page 14)

A Flexible Data Model for the National Capital Region Critical Infrastructure Protection Project

Anoop Singhal and Sushil Jajodia
Center for Secure Information Systems, George Mason University


Anoop Singhal

A principle component of the National Capital Region Project will be the development of a flexible data model and database. These tools will be essential to the storage of vulnerability assessment data and key to the process of evaluating the assessment data collected.

Data to be incorporated into the data model will include a detailed range and depth of information from previous vulnerability assessments. This data will then be modeled by the Data Modeling Team in an Object Relational data model using Rational Rose Data Modeling Tool. It will be stored in ORACLE 9i database system that can be queried in order to do an evaluation of the assessment data and develop best practice auditing tools and a framework for future infrastructure vulnerability assessments. We will first baseline the current infrastructure information. This information can also be used for emergency preparedness and first response needs in the event of chemical, biological and nuclear incidents.

We plan to use data warehouse technology to store the critical infrastructure information and then design separate data marts for each critical infrastructure, initially focused on Transportation, Energy, and Telecom. The main benefit of a data warehouse is that it will contain all the information in one central place and a common data model which the users can query and analyze. Each of the data marts will provide a subset of the information that is of value
(Continued, Page 14)

LEGAL INSIGHTS

by Emily Frye

Protection Strategy: Territorialism or Regionalism?

One of the biggest challenges to effective national Critical Infrastructure Protection is this: threats don't come in neatly defined bundles, but legal jurisdictions do. To understand the implications of this assertion, it is only necessary to recall the contrast between the attacks on New York's World Trade Center and the attack on the Pentagon. The Twin Towers sat within New York City, within New York State. Authority - and responsibility - to respond fell to New York City first, and then to New York State. As a nation, the response came in droves from a large number of jurisdictions, but authority was clear. [Port Authority?]

By contrast, the Pentagon sits in the Commonwealth of Virginia, yet is property of the federal government. While emergency response fell to local area teams, the federal government quickly became involved in reconstituting function and generating the repair strategy. The Pentagon cleanup protocol provides a less-common example of federal control inside a sovereign state.

To understand why this is so, it is instructive to consider the nation's origins. Having just fought to free themselves from a distant and centralized ruling structure, it was only natural that the thirteen states began discussion of nationhood with some trepidation. In fact, it took until the Convention of 1789 for the states to decide they were willing to get "married" (form a Union) instead of live together (in Federation). Even so, the (10th Amendment of the) Constitution explicitly reserved to the states the right to govern all matters not set aside for centralized management. Two centuries later, states continue to have extensive rights to self-government; in many ways, they retain control of what happens within their borders. In most cases, this makes sense: states are most familiar with their own citizenry, local culture and preference, geological and geographical peculiarities, and a myriad of other details that contribute to effective governance.

Recall, after 9/11, the overwhelming outpouring of support in New York City from First Responders and the public - not just from the citizens within the City or the State, but from all across America. Those who visited in the months after the bombing saw clean-up crews from virtually every state and territory. The state and the city coordinated these workers in the months following the attack to clear the rubble and ruin. Although the response was national, the authority was local.

Unlike New York, the authority for the Pentagon was not purely local, but involved cross-jurisdictional authorities for response and clean-up. Local county fire departments were involved at the beginning because the federal government does not maintain those types of capabilities. Subsequently, clean-up and rebuilding authority was transitioned to the federal government. It, too, had to coordinate workers who traveled hundreds of miles to participate in the "Phoenix Project," to ensure the building was restored by the first anniversary of the attacks. But in contrast to New York, the feds had the added responsibility of repairing a building within another sovereign's jurisdiction.

Most recently, the Northeast Blackout showcased the ability of any number of jurisdictions to work together when all were affected. But consider another type of disaster - one, say, in the Four Corners region of the West, where Arizona, Colorado, New Mexico, and Utah come together. A chemical spill at a northern Arizona plant would fall soundly within Arizona's traditional jurisdiction - yet the consequences would affect residents of four states. Assume that New Mexico, but not Arizona, has a toxic-substance cleanup crew. Does Arizona have the right to call in the New Mexican expertise? If the spill leaks into New Mexico, does the New Mexican crew have the obligation to treat the damage in its home state before the damage in Arizona, even if conditions are more dire in Arizona?

These questions highlight the reality of modern-day threat planning.
(Continued, Page 14)

Critical Incident Analysis Group and Community Shielding Concept

The Critical Incident Analysis Group (CIAG) is a division of the Center for the Study of Mind and Human Interaction in the University of Virginia's School of Medicine. CIAG is an interdisciplinary consortium of academicians, professionals, and experts dedicated to improving the public's ability to understand and cope with "critical incidents", and government's capacity to anticipate, prevent, and manage them effectively. A critical incident has the potential to cause personal trauma and undermine social trust, creating fear that may have impact on community life and even on the practice of democracy. CIAG brings together professionals concerned about the profound impact of critical incidents, drawing on the expertise of physicians, social scientists, medial researchers, law enforcement specialists, policy makers, diplomats, philosophers, military leaders, historians, journalists, and writers, among others, to analyze critical incidents and to find ways to prevent new ones from occurring. To date, CIAG has focused attention on time-limited, newsworthy, provocative events, such as the siege in Waco, the bombing in Oklahoma City, the Exxon Valdez oil spill, the attack on U.S. embassies in Africa, Aum Shinrikyo, Community and Public Health Response to the West Nile Virus, the attacks on the World Trade Center, the attack on the Pentagon, bioterrorism hoaxes, the anthrax attacks through the U.S. mail, and most recently, the Northeast blackout.

Within the context of the NCR Project, Gregory B. Saathoff, M.D., Executive Director of the CIAG, and his team will contribute their expertise on the elements of social dynamics of crisis response, looking across the critical infrastructures within the national capital region to develop a model for the community shielding concept. This concept is defined as 'a form of insulation wherein individuals and groups employ a self-imposed isolation, or quarantine, within their natural surroundings for a temporary period of time. This concept is an alternative strategy that could be used in concert with other possible responses following a bioterrorist attack, such as mass quarantine or spontaneous evacuation. While mass quarantine is a coerced, reactive top-down, involuntary measure imposed by government, and spontaneous evacuation represents a chaotic dispersal of persons and bioterror agents, community shielding represents a facilitated, proactive, bottom-up voluntary approach sanctioned by government. Recently, the International Journal of Emergency Mental Health (vol. 4, no. 4, Fall 2002), devoted an entire issue to the community shielding concept through the lens of law, political science, communications, mental health and public health. The concept has also been described in the Wall Street Journal and the Chronicle of Higher Education. Earlier this year, Virginia's General Assembly passed House Joint Resolution no. 924, commending the Critical Incident Analysis Group of the University of Virginia for developing the concept as an important effort in protecting America's communities from terrorist attack. ❖

Gregory Saathoff

"It is a privilege to be part of the National Capital Region Project. The public rightfully expects universities to collaborate to develop strategies for safety and security in the interest of the public good, while preserving civil liberties. The interstate academic consortium that makes up the NCR project is the type of network that is necessary for the creative collaboration that society requires."

Frank Sesno, Senior Fellow to the CIP Project, talks with Michael Byrne, Director of the Office of National Capital Region Coordination for the Department of Homeland Security

SESNO: Let's start by talking about the recent power outages, the big one on the East coast and the outages caused by Hurricane Isabel, with regard to specific lessons learned that apply to Homeland Security?


Michael Byrne

BYRNE: Yes, absolutely. I think it is just a reminder of how linked we are and how dependent we are on so many things that require power. The things that struck me most were the connections with the water systems - when we lost power, we lost water, we lost sewage treatment and those cascading types of effects had probably a larger impact than people envisioned. This was a real wake-up call for people. I also think it was a reminder that we're really serious about individual preparedness. I spoke with a lot of elected officials and I asked them, "What kind of calls were you getting during these events?" And the calls they were getting were people who had not put away some water, that had not bought a manual can-opener to open canned food, they had not done any kind of preparation that we had been asking people to do for two years now. And this was like a wake-up call to say, "Hey, we are serious about this."

As a society, we have become too overly reliant on systems that can fail. Mother Nature is still going to send us a curveball every now and then. We are human, things will happen that will have an impact, and we need to have a greater degree of self-reliance.

SESNO: Are specific steps being taken as a result of the lessons from these recent incidents?

BYRNE: Definitely. On the energy side from the blackout, much of the investigation is going into why it happened and what kind of redundancy can be built into it. I think Isabel is even generating more of a discussion about what are prudent levels. We can never protect things 100%, but Isabel is starting a dialogue that was probably well underway but has gotten more force as a result, and that is that how much should you prepare. One thing about Isabel though, when you don't have power its unbearable and we need to have some reliance, people should have the sense that their power is reliable, that their power is going to be there when they need it. But I think we also need to take a look at the robustness of our system.

At the height of Isabel we had 4.85 million people without power. That is an incredible number.

By Monday morning following the event, 74% of the people who did not have power at the height of Isabel had their power restored. That is an incredible achievement. In this country, that we can get teams out there while trees are still falling, while water is still rising, while all of that is still going on, that we can still get good people out there to restore power. To the extent where ¾ of the people have power, that is significantly robust.

I think as we move on from that, as we get into weeks down the road we'll recognize that we are doing some things right already. But, what else do we need to do? What other kind of things do we need to do?
This is not the first hurricane we have had where this kind of dialogue has started. It's when the idea of buried utilities comes up, the idea of different kinds of redundancies comes up. I think now a combination of a recent natural hazard combined with our interest in protecting ourselves because of the threat of terrorism. We have the opportunity to make those kinds of prudent judgments that are necessary.

SESNO: Let's turn to the Urban Area Security Initiative. It's a project that will among other activities attempt to assess all infrastructures in the National Capital Region, sort of a test bed
(Continued, Page 9)

Byrne / Sesno Interview *(Cont. from Page 8)* for better preparations across the board, across urban areas into the future. Describe the project.

BYRNE: The Urban Area Security Initiative is a really exciting opportunity because for the first time, funding is not specifically tied to an individual state or an individual jurisdiction, but is actually tied to an entire region which crosses two states and the District of Columbia, which makes it a special kind of region.

And it provides us with an opportunity where in the past, if you wanted to do something jointly, you had to go to each jurisdiction and say "What can you bring to the table? How much funding or resources can you put behind a joint effort?" This is by definition a joint effort and a collaborative effort.

As is, our critical infrastructure is not something that stops at state lines, at the district line; it is something that we share across these jurisdictions, across the jurisdictions within the communities. This funding allows us to focus attention and to reap a benefit from that.

SESNO: What is the goal of the project?

BYRNE: The goal of the project is to be able to study and look at not only each of the critical infrastructure areas but also to look at the dependencies and the connectedness that these have on each other, as was demonstrated in Isabel.

Our guiding principles are the President's Strategy on Critical Infrastructure. The information in there is what we will follow in terms of what questions we need to ask and what results we are looking to get out of it.

At the other side of this, what I am hoping is to have, what I think all of us are hoping for, is clear, deliberate steps that we can take to both better protect our infrastructure and also to be better able to respond should we have either a natural disaster or a terrorism incident.

SESNO: Specifically, what do you most hope that you will learn from this?

BYRNE: I think what I am really hoping for is that we recognize the interdependencies that exist. Whether they be just purely communication, whether they be hardwired disconnects that happen as a result of something going down.

Right now, power and water are on very much on everybody's mind but if we look to the other critical infrastructure areas, if we look to health care or emergency services, for example, the reality that we face and we are lucky to be in the region we are in because there is a great deal of collaborative effort that goes on here. It's endemic in this area. But, it is not everywhere and what we should be able to show is how that works. How, from a critical infrastructure point-of-view, can the health community, the emergency services community, and the telecommunications all be linked together and in line with the President's Strategy for Homeland Security and the idea of National Incident Management System, so that we end up identifying those basic things that we all have to have in common so that we can even talk to each other and support each other in times of crisis.

SESNO: Do you anticipate specific challenges or problems as infrastructure owners and providers are bolted into this process, further engaged into through the inquiry and initiative?

BYRNE: I think we will go through a very expected sort of time period of building trust. We have made a good deal of progress in that in the last two years. We are fortunate in this area to have utility companies, to have infrastructure-related companies that understand the issues and are willing to come to the table.

I think we still need to build a sense of trust about the information, a sense of trust about kinds of products and recommendations that will come out on the other side of this effort.

SESNO: How will you apply the information that you gather in a practical sense to enhance homeland security?

BYRNE: From a practical sense, ultimately that's really what we are looking for. It would be really nice to have all of these wonderful theoretical documents out *(Continued, Page 14)*

James Madison University and the National Capital Region Project

As part of the close partnership with George Mason University, James Madison University will provide a vital link in the early stages of the National Capital Region (NCR) Project. Under the leadership of Dr. George Baker, Associate Professor within the Department of Integrated Science and Technology and the Associate Director of the Institute for Infrastructure and Information Assurance (IIIA), the JMU team will be responsible for data gathering as well as assessing and integrating vulnerability assessment frameworks. Drawn from critical infrastructure sectors such as energy, telecommunications and transportation, the collection of vulnerability data will be a key part of the process of identifying a best practice assessment tool. In addition, Dr. Baker's experience with vulnerability assessments will be translated into the training and methodology needed by the field research teams as they begin data collection and analysis of the existing assessments.

Dr. Baker brings significant leadership and expertise to JMU and IIIA as he previously directed the assessment division within the Defense Threat Reduction Agency (DTRA) and was responsible for assessing and protecting critical Department of Defense (DoD), North Atlantic Treaty Organization (NATO), and national infrastructure facilities. Dr. Baker has continued to develop a risk assessment model for critical infrastructures through his work with the Critical Infrastructure Protection Project at James Madison University. Ms. Jessica Milloy has joined the NCR team as JMU's lead representative on the project. In this role, Ms. Milloy will work closely with the field teams conducting the assessments and will also serve in a training capacity with Dr. Baker. ❖

Risk Management and the NCR Project: Virginia Tech and the University of Maryland to Examine Interdependencies


Gregory Baecher

The Center for Disaster Risk Management (DRM/VT) at Virginia Polytechnic Institute and State University (Virginia Tech) will be a key collaborator on the NCR Project, under the leadership of Dr. Frederick Krimgold, Director of the DRM/VT. DRM/VT, in collaboration with Dr. Gregory Baecher, Director of the Center for Infrastructure Risk Management, Economics and Security of the University of Maryland has carried out an initial survey of critical infrastructure vulnerability assessments in the National Capital Region under the auspices of the Metropolitan Washington Council of Governments.

DRM/VT is the US component of the World Institute for Disaster Risk Management (WIDRM), an initiative of the Board of the Swiss Federal Institutes of Technology and Virginia Tech in conjunction with the ProVention Consortium of the World Bank and Swiss Re. WIDRM is a network for applied research, implementation, and dissemination in the field of disaster risk management. The objective of DRM is to enable people to anticipate disasters and take action to protect life and property, and to ensure sustainable social and economic development. Its activities include supporting the pursuit of an optimal balance between *(Continued, Page 11)*

Dr. Krimgold is very enthusiastic about the broad interdisciplinary collaboration and the cooperation of public and private organizations in the NCR Project. "This project has the potential to expand our fundamental understanding of how urban systems work and to make a major contribution to sustainable urban management. The recent experience of the Northeast Blackout and the impact of Hurricane Isabel can provide an excellent learning experience for the broader topic of infrastructure security."

Critical Infrastructure Modeling and Assessment Program Elements

The first element strives to examine the infrastructure security in the Washington metropolitan region. As researchers become familiar with the area, they are able to assess regional vulnerabilities, and identify, as well as prioritize, infrastructure interdependencies for protection and damage control.

The second element, electric power transmission line monitoring, analyzes data to determine the risk of cascading failures that lead to blackouts. The element also includes monitoring for early detection and warning signs of relay failures.

Enhancing power quality and security of supply is the third element. The concept refers to identifying alternative energy sources for reliability in emergencies.

The fourth and final element is data visualization. CIMAP creates graphical representations of large amounts of data to help the viewer understand and interpret the big picture for a given area.

Key faculty participants in CIMAP include Dr. Saifur Rahman, Dr. Michael Willingham and Dr. Lamine Mili.

Risk Mgmt & NCR *(Cont. from Page 10)* disaster risk reduction, risk-sharing mechanisms, and management of residual risks in the face of finite resources.

DRM/VT has carried out significant research and development projects in the area of natural disaster vulnerability reduction. Currently, work is being completed on a series of manuals for building owners and structural engineers on "Incremental Seismic Rehabilitation of Commercial and Institutional Buildings". A recent FEMA publication completed by DRM/VT addresses "Insurance, Finance and Regulation for Terrorism Risk Management in Buildings." DRM/VT has also been actively involved in disaster risk management project work in India, Turkey and Mexico under the auspices of USAID and the World Bank. DRM/VT brings to the NCR project other strengths of the Virginia Tech faculty through the Critical Infrastructure Modeling and Assessment Program (CIMAP) undertaken by the Virginia Tech Center for Energy and the Global Environment (CEAGE) to assess critical infrastructures in Northern Virginia. The aim of this program is to provide state policy-makers and legislators - along with citizens, state and federal agencies, and industry partners - with long-term perspectives and guidance on the various issues that affect the planning, commissioning and operation of infrastructures, and to provide an early identification of events and trends that may have a potential impact on the capability of utility infrastructures to provide service in a timely, economic, and environmentally sound manner. CIMAP focuses on analyzing the changing demands on individual infrastructures, examining how these demands are leading to greater infrastructure interdependencies, and determining how these demands and interdependencies will in turn affect their capability and availability.

Michael Willingham

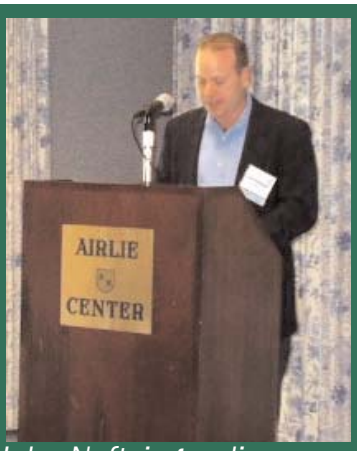
Saifur Rahman

Collaboration between Virginia Tech and the University of Maryland has been invaluable in the development of a comprehensive characterization of infrastructure vulnerability for the National Capital Region. The University of Maryland Center for Infrastructure Risk Management, Economics and Security includes key faculty from engineering, planning and public policy. Dr. Gregory Baecher has extensive experience in water systems risk analysis. Dr. Jacques Gansler has broad experience in national security policy at the highest level. Dr. Phillip Tarnoff is the Director of the Capwin project for emergency communications in the National Capital Region.

The contribution of the Virginia Tech/ University of Maryland *(Continued, Page 13)*

CIP Project Airlie House Workshop

The CIP Project is proud to announce the publication of its first collection of working papers. Coming in late September, the book features 31 complete papers and "works in progress" from GMU and JMU scholars, as well as academics from other universities. As an accompaniment to the book, the CIP Project has also created a CD ROM that provides a comprehensive overview



John Noftsinger discusses the ongoing collaboration of James Madison University.

of the critical infrastructure protection arena. Highlighting policy and technology foundations, the CD provides a primer on critical infrastructure protection and is an excellent source of key information. The CIP Project hosted a comprehensive workshop to celebrate the book's publication, allow researchers to present their papers, and provide the opportunity for CIP Project staff and researchers to get to know each other better.

Held over September 15-16 at the Airlie Center in Warrenton, Virginia, Law School Dean Mark Grady opened the Workshop and welcomed participants. Grady was followed by a CIP Project Update by Associate Directors Kip Thomas and Emily Frye. Thomas and Frye were proud to report that the CIP Project has sponsored over 50 research projects to date, representing nearly $10 million in grant funds. Overall, the CIP Project has sponsored research at 14 universities, with 77 scholars, and over 200 undergraduate and graduate students.

With that introduction, the research presentations began. The presentations were organized according to discipline: Cyberspace Critical Infrastructure Protection, Real-Space Critical Infrastructure Protection, Government Regulation, and Private Regulation. In addition, three specially selected student presentations capped off the end of the first day and their papers were also included in the workshop published proceedings. For some, this type of presentation was a first, and represented a unique opportunity for peer review and critique.

Kip Thomas provides an update on the CIP Project

Roy Rosenzweig, Tom Scheinfeldt, Kathi Ann Brown and Rebecca Luria give a preliminary report on the Critical Infrastructure Protection Oral History Project.

Many participants commented on the great progress being made by the CIP Project, as reflected by the Off-Site. "This CIPP research workshop is the most fruitful cross-university exchange that I have seen since coming to GMU in 1990," said Roger Stough, NOVA Endowed Chair and Professor of Public Policy. "The CIP Project and staff should be complemented for creating such a great environment for research and idea exchange." Christopher T. Hill, Vice Provost for Research, added, "There was a palpable sense of both intellectual excitement and commitment to solving important national problems in the room. . . I look forward to the next get-together when the promises and approaches of this meeting will have *(Continued, Page 13)*

McCarthy Testimony *(Cont. from Page 3)* token, sufficient safeguards and incentives must be structured for all stakeholders to fully participate in the process. As a former first responder and trained incident commander, I believe management of these complex social response networks at all levels of the federal response structure will be increasingly important in the successful resolution of infrastructure incidences of national significance, be they physical, cyber, or both. The establishment of a public-private liaison as a senior advisor to Secretary Ridge is an important and needed step in developing and advancing this emerging need.

These two Committees have chosen to address these issues at the right time, and I commend you in holding this hearing. The CIP Project's primary goal is to match scholarly research with the real-world issues and problems faced by industry and government leaders at this important time in our Nation's history. With your continued support, the academic community can continue to provide unique fora to assist decision-makers in discussing and developing solutions to these pressing issues.

Thank you. I look forward to answering any questions you may have. ❖

Risk Mgmt & NCR *(Cont. from Page 11)* team to the NCR project is a direct response to the Eight Commitments to Action of the August 2002 NCR Homeland Security Summit. As a part of the NCR project, particular attention is focused on Commitment number 5: "Infrastructure Protection." Based on the experience of earlier survey and analysis the team will work with the private sector to jointly identify and set protection priorities and guidelines for infrastructure assets and services in the National Capital Region.

The principal focus of the DRM/VT component of the NCR project will be the analysis of critical infrastructure system interdependencies. One of the principal findings of the earlier research carried our by DRM/VT for the Council of Governments was that each infrastructure sector had initiated some form of vulnerability assessment but these assessments were uniformly limited to the internal vulnerabilities of the particular system. Little attention has been paid to cross-system interactions and interdependencies.

The initial work of DRM/VT will be to collaborate with the principal providers of energy, transportation, communications and water and sewer to identify critical interdependencies. ❖

Workshop *(Cont. from Page 12)* led to important advances in understanding and in future directions for the United States."

Day 2 of the conference centered on Real Space Critical Infrastructure Protection and Government Regulation. The conference was closed with brief remarks by John McCarthy, CIP Project Executive Director. McCarthy commented that, when asked if his misses being involved in the government and homeland security issues, he replies "No, because the research agenda being developed across JMU and GMU is as important as any work I did during my government career."

Copies of the all presentations made at the off-site will be posted on the CIP Project website. ❖

Information Sharing *(Cont. from Page 5)* occurred. For instance, how have the project teams interfaced with each industry to be able to collect the data they need to assess different models of vulnerability assessment? What specific methods of information gathering were most effective? Compiling these best practices will allow us to cultivate a model for best information sharing practices, along with specific policy recommendations for achieving high levels of collaboration within the NCR project. ❖

Flexible Data Model *(Cont. from Page 5)* to a specific group of users in each industry area. We also plan to use data mining and data visualization tools that can help the user analyze data and discover knowledge about the vulnerability assessment data. ❖

Byrne / Sesno Interview *(Cont. from Page 9)* there, but what we really would like to see is projects with steps to them that can have demonstrable improvements to the critical infrastructure reliability and capabilities.

What we are hoping for is that we are able to balance the information we get with what I like to call just prudent judgment that we as a community can say, "Yes, this is the level of redundancy, this is the level of protection, this is the level of preparedness that we're willing to embrace." And should that not be enough, that there will be other ways for us to manage while the infrastructure is restored. ❖

Legal Insights *(Cont. from Page 6)* Although the country grew up on state sovereignty and state responsibility, it is now time for a profound rethinking of roles and obligations that transcend traditional boundaries. One of the reasons the National Capital Region project is so important is that it begins to make these categorical leaps - to move beyond geographical, legal boundaries to realistic threat evaluation. And realistic threat evaluation means acknowledging that threats have no respect for state lines. ❖

The CIP Project is part of the National Center for Technology and Law at the George Mason University School of Law. It is a joint initiative between GMU and JMU that examines law, technology, and policy to find comprehensive solutions to the most pressing CIP issues for policy makers and critical infrastructure owners and operators. The CIP Project was launched in May 2002. The CIP Project encourages participation by representatives from all levels of government, academia, and private industry.

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Project. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for The CIP Report, please click on this link: http://listserv.gmu.edu/archives/cipp-report-l.html.