OCTOBER 2004 / VOLUME 3, NUMBER 4

THE CIP REPORT

CIP Program Offsite

CIP Program Staff

John McCarthy, *Director / Principal Investigator*

Jerry Brashear, *Associate Director, National Capitol Region Project*

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

Rod Nydam, *Associate Director, Private Sector Programs*

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

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

Contact: cipp01@gmu.edu
703.993.4840

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

A Message from John McCarthy:

As many of you know, we recently celebrated an important milestone for the CIP Program during our Second Annual Offsite at the Airlie Center. This event not only provided an opportunity for our researchers to present and discuss their funded projects in a forum open to dialogue and constructive questioning; it allowed all of those involved to see the diverse, interdisciplinary, multi-institutional and highly collaborative nature of the CIP Program as we enter our third year.

While I was unfortunately unable to attend the event due to an extended medical leave, I would nevertheless like to take the time to comment upon the event and thank those who participated and organized the event. I greatly appreciate the presence of our JMU partners, and in particular, Dr. John Noftsinger, Associate Vice President for Academic Affairs, and Dean A. Jerry Benson, for providing their welcoming remarks to set the tone for the event. I would also like to thank the leadership at GMU, such as Vice Provost Chris Hill for his attendance, and Dean Dan Polsby of the Law School for his closing remarks, which served to further challenge and engage our researchers to consider unexplored areas of critical infrastructure protection. I would also like to thank Steven Simon, a CIPP Senior Fellow, for his fascinating keynote address during dinner that held everyone spellbound right up to the start of the first Presidential Debate. Finally, an event of this magnitude would not have been possible without the tremendous effort of individuals such as Christine Pommerening, Amy Cobb and Emily Frye.

As we take this moment to reflect upon the importance of this event, I would like to encourage everyone to continue the dialogue and conversations begun during the questions following presentations, during breaks or over dinner. While this event provided an opportunity to showcase and present our work, it also provided an important opportunity to initiate interaction with peers at different institutions and colleagues in related fields. These conversations should and must continue to further push our work to new levels and strengthen the interdisciplinary and collaborative nature of our Program.

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

We were also very proud to present the release of the second volume of CIP generated research, *The Critical Infrastructure Protection Program Workshop II Working Papers*. This new publication moves beyond many of the preliminary papers included in last year's volume, and provides more substantive examinations of the research funded at 15 different universities, by over 70 researchers and involving over 200 students. As our Program grows, our research matures, and new projects, researchers and students are added to our portfolio, these books will continue to provide a lasting legacy of the vital work undertaken by this group.

This month's edition of *The CIP Report* provides an overview of the research presented, captures some of the important conversations begun and shares the perspectives of those who attended.

Second Annual CIPP Researchers' Workshop Addresses Progress Made and Challenges Ahead

Christine Pommerening, George Mason University

When over 60 CIPP researchers gathered in Warrenton, Virginia, for the second annual offsite workshop on Thursday, September 30th, 2004, everyone was acutely aware of the increasingly political disputes about the right ways to protect the nation. It happened to be the night of the first Presidential debate between George W. Bush and John F. Kerry, and fittingly enough, the topic here as well as there was homeland security.

The retreat started with welcoming remarks by Jerry Benson, Dean of the College of Integrated Science and Technology at James Madison University. He highlighted the evolution of critical infrastructure protection into a widely recognized issue for academic research and development in a variety of disciplines, and the evolution of what started out as a bilateral project into a multi-institutional program.

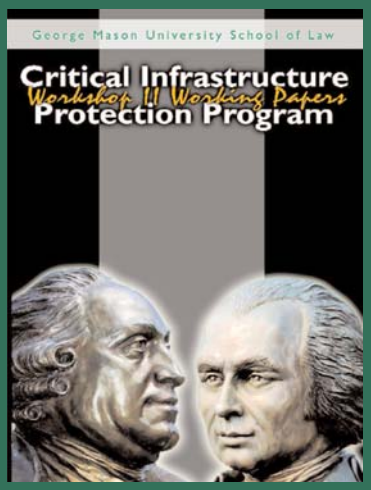
The workshop itself was organized into 10 panels with a total of 35 presentations and demonstrations, and ample opportunity for discussion with the audience. The panel members and moderators took the opportunity to make this a truly interactive workshop--one sign of the growing understanding of each other's work and collegial atmosphere throughout the program.

The workshop was indeed designed to bring together different disciplines and methods, and identify connections and common themes between projects that range from local to international infrastructure protection issues, from software to building architecture, and from constitutional law to organizational theory perspectives. While many of these issues seem to be only marginally related, the contributions and panel discussions revealed that all four core disciplines of law, economics, engineering, and public policy need to be considered in the analysis of critical infrastructures, and especially in the development of any recommendation or application.

The six panels on the first day dealt with civil and systems engineering; transportation; business information; states, markets, and networks; insurance and assurance; and civil rights.

Civil and Systems Engineering

In the first panel, David Schum sketched out a logic framework for integrating evidential reasoning and evolutionary computing that can aid in generating terrorist scenarios. Using a similar evolutionary computing approach to scenario generation, but on a different level of abstraction, Mo Wadda gave some practical insights into protecting water distribution systems. The last presentation also dealt with water supply, but from a geo-spatial point of view. Tim Evans introduced work recently begun on using Geographic Information Systems (GIS) to protect water supply in karst geology.



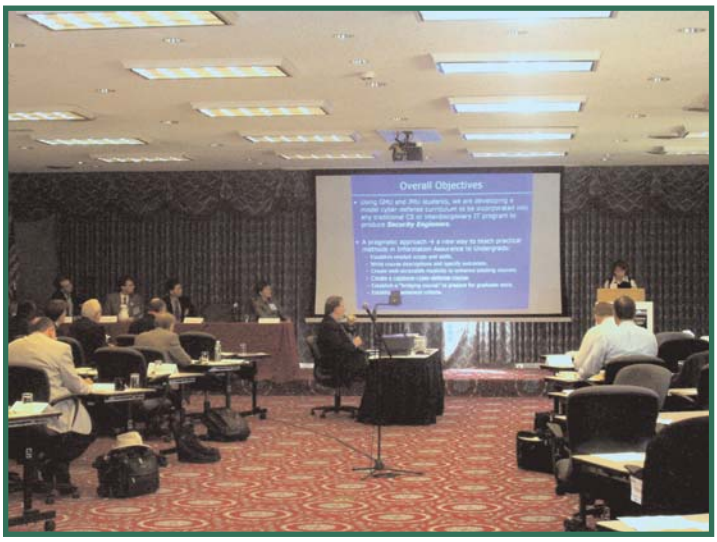
CIP Program Workshop II Working Papers

Expertly moderated by Tomasz Arciscewski, this panel demonstrated how engineering and information sciences contribute to understanding threat conditions.

Transportation

The second panel, chaired by Christine Pommerening, brought together three experts on storage and transportation-related issues. *(Continued, Page 3)*

Overview *(Cont. from Page 2)*
Helmut Kraenzle described a geographic information system for simulating container movement (GISSCM) that can be expanded to worldwide end-to-end tracking not only of the containers, but its contents. Michael Bronzini then highlighted technologies and devices that enable the identification of vehicles, operators, and cargo for surface transportation. Finally, Michael Deaton outlined elements of a decision support system for hazardous materials (HAZMAT) storage sites in communities; illustrating the continuing problems in adequately securing those sites with a short video clip on the ease of access to a chemical plant.



Anne Marchant of GMU discusses building undergraduate curricula in security.

The contributions illuminated the challenges our highly integrated and mobility-dependent society faces, where distance has lost some of its prohibitive and thus protective qualities.

Business Information and Decision Making Systems

The third panel dealt with business information and decision-making systems. Moderated by Emily Frye, the presentations showed the criticality of information and communication for companies involved in infrastructure and service provision. Geoffrey Egekwu proposed a security-focused assessment method for Supervisory Control and Data Acquisition (SCADA) systems that recognizes the so-called vulnerability triangle between hardware, software, and people. The many factors to be included in a comprehensive vulnerability assessment were also addressed by George Baker, who has developed a methodology that takes into account the mission-critical systems that make up individual critical infrastructure facilities. Kevin McCrohan then emphasized the role of management in a cyber-dependent economy. Information security needs to be understood as a managerial imperative, not just a technical issue, and communicated and implemented as such.

In addition to the panels, there were two demonstrations of new software systems. Bill Tulloh and Jack High are working on a beta test version of an operating and desktop management system that eliminates many of the authentication problems embedded in current off-the-shelf programs. This new software code can help protect property rights and prevent virus attacks. Rafal Kicinger displayed an integrated computer tool called “TerrorMax /Capitol Hill", which demonstrates the potential of a proactive security approach in the context of critical infrastructure protection. The system is intended for the evolutionary generation of terrorist scenarios for the Capitol Hill area of Washington D.C., and includes a Flash visualization module for scenario animation.

States, Markets, and Networks

In the afternoon, panel four with moderator Christine Pommerening convened to discuss various issues relating to the response and behavior of states, *(Continued, Page 4)*


Jerry Benson, Robert McKown, and Ronald Raab of JMU

Overview *(Cont. from Page 3)*
markets, and networks facing criminal and terrorist threats. Ted Woodcock introduced different modeling and simulation support programs that can be used in the new security environment ranging from troop deployment to peace operations to humanitarian aid. Stephen Bowers presented findings on the factors contributing to cyber crime in Romania, in particular the communist legacy and post-communist instability. Finally, Brian O'Roark analyzed the shifting equilibria between marginal costs and marginal benefits of security measures when complications such as expected value and uncertainty, distributed decision-making and externalities, and litigation are taken into account.

Insurance and Assurance

Panel five, again knowledgeably chaired by Emily Frye, explored insurance and assurance as mechanisms for improving preparedness. Michelle Boardman contended that recent government efforts of mandating terrorism insurance cannot work because of unknown risk distributions. Moreover, the pretense of insurability of major losses prevents the development of a market for moderate risks. A different approach was presented by Anne Dailey, who reported on a more bottom-up model of a voluntary industry association for assuring the energy grid. Similarly, Jane Winn proposes a self-regulatory strategy to increase investments in computer security. A combination of compliance reporting and trade practices law seems to be an alternative to direct government intervention.

Christine Pommerening of GMU moderates a panel on transportation.

Individual and Collective Rights

The final panel of the day was moderated by Ken Newbold, and concentrated on individual and collective rights and decisions. Ross Davies examined how the rights to strike, lockout, and replace can be preserved in an age of terror threat. He argued that adopting a waiting period legislated since 1974 for the health care industry can be used in other critical infrastructure sectors to prevent opportunistic exploitation of labor disputes while protecting workers' and managements' rights. Ilya Somin outlined the relationship between political ignorance and the war on terror, claiming that the general tendency of voter inattentiveness to complex subject matters might lead to unwise political decisions. The last speaker, Farrokh Alemi, put forward a proposal for a national database of incidences of privacy violations that rests on the probabilistic analysis of risks instead of perceived or even imagined vulnerabilities.

Michelle Kaarst-Brown of Syracuse and George Coffman of JMU

The two-day event continued on Friday, October 1st, with four panels, focusing on local and international issues; biodefense; cooperation and coordination; and social and organizational aspects.

Local and International Issues

The first panel of the day, and seventh overall (and third one moderated by Emily Frye), featured four reports that demonstrated how much seemingly local phenomena are connected to global trends, and vice versa, and how national and international legal and economic systems intersect. Randy Jackson outlined a new project that will compile and compare the CIPP-relevant legal and regulatory provision *(Continued, Page 5)*

Overview *(Cont. from Page 4)* in several countries into a searchable database. Willem Holleman, an international CIPP fellow from the Netherlands, then talked about how port security is a global goal but with very distinctive, and sometimes diverging approaches. For example, in many European countries, port security is predominantly perceived as a safety issue rather than a terrorism problem. This difference in perception is important, because protective measures and enforcement vary accordingly, but still need to be standardized to some degree in ports around the world. Like ports, shopping malls represent an interesting subset of highly integrated yet somewhat exclusive systems. Marc Thibault explained that the physical layout and logistics of shopping malls make them vulnerable to attacks; for example, the convenience of adjacent parking is achieved at the cost of security. Shopping malls are integral parts of urban and suburban neighborhoods, and in fact serve as anchors for new housing subdivisions. One of the implications of living in such multi-functional communities is the need for communication among all kinds of individuals, groups, organizations, and institutions for disaster response. Roger Stough's presentation reviewed alternative telecom network options, and proposed a web-based solution to this problem called ReadyLinks.

Dean A. Jerry Benson of JMU welcomes workshop participants.

Biodefense

The eighth panel examined some medical, physiological, and engineering aspects of defending against biological threats. Arnauld Nicogossian emphasized that protecting the nation's blood supply is both a medical and a policy problem since collecting, processing, and distributing blood involves all actors in the health policy field, from legislators to physicians to donors. Ronald Raab then described his project, which aims at identifying and developing recombinant biological vaccines and critical diagnostics to address biological agents that could be used by terrorists. Finally, Gene Tucker showed an actual, barely palm-sized air quality sensor that was developed by his team for use in various indoor alert and alarm systems.

Josh Barnes, Ken Newbold, and Ben Delp of JMU

Cooperation and Coordination

The penultimate panel, chaired by Rod Nydam, addressed cooperation and coordination issues, and more importantly, models for solution. First, Anne Marchant reported on the successful implementation of initial modules for a security curriculum for undergraduate students in information technology and engineering. While there is much promise, there are also administrative and institutional challenges before implementing a comprehensive program of study. A similar mix of success and challenge is faced by university consortia and their managers, and Ken Newbold suggested ways to get a grip on these kinds of strategic alliances. A more theoretical perspective was offered by Amitai Aviram, who examined the evolution of private associations for cyber-security as an instance of a non-market, non-hierarchical response to a common threat, or in other words, of network responses to network threats.

Rounding out the panel was an account of *(Continued, Page 17)*

2nd Annual CIPP Offsite Workshop
September 30 - October 1, 2004 Warrenton, VA
AGENDA

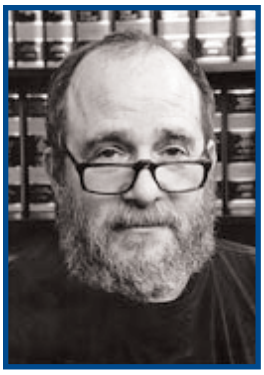
Thursday, October 30			
8:30 - 9:00 a.m.	Check In		
9:00 - 9:15 a.m.	Welcome		Dean Jerry A. Benson, JMU
9:15 - 9:30 a.m.	CIP Program Update		Emily Frye, GMU
9:30 - 10:15 a.m.	Panel I	Civil and Systems Engineering	Moderated by: Tomasz Arciszewski, GMU
	1	Generation of Terrorist Scenarios: Integration of Evidential Reasoning and Evolutionary Computing	David Schum, GMU
	2	Generation of Terrorist Scenarios for Water Distribution Systems: An Evolutionary Computation Approach	Mo Wadda, GMU
	3	Geographic Information System Application to Water Supply Protection in Karst Geology - An Introduction to Work Recently Begun	Tim Evans, JMU
10:15 - 11:00 a.m.	Panel 2	Transportation	Moderated by: Christine Pommerening, GMU
	1	Geographic Information System for Simulating Container Movement (GISSCM)	Helmut Kraenzle, JMU
	2	Technologies for Vehicle, Operator, and Cargo Identification	Michael Bronzini, GMU
	3	HAZMAT Decision Support System	Mike Deaton, JMU
11:00 - 11:15 a.m.	Break		
11:15 - 11:45 a.m.	Demonstration	Software Codes, Property Rights, and Virus Attacks	Jack High and Bill Tulloh, GMU
11:45 - 12:45 p.m.	Panel 3	Business Information	Moderated by: Emily Frye, GMU
	1	Assessing SCADA Systems: An Update and Proposal	Geoff Egekwu, JMU
	2	Management's Role in Information Security in a Cyber Economy	Kevin McCrohan, GMU
	3	A Vulnerability Assessment Methodology	George Baker, JMU
12:45 - 1:45 p.m.	Lunch		

Thursday, September 30 (Continued)			
1:45 - 2:45 p.m.	Panel 4	States, Markets and Networks	Moderated by: Christine Pommerening, GMU
	1	Risk Assessment Models for the New Security Environment	Ted Woodcock, GMU
	2	Cyber-Crime in Romania: Problems and Responses	Stephen Bowers, JMU
	3	A Threat-Response Model of Counter-Terrorism: Implications for Information and Infrastructure Security	Brian O'Roark, JMU
2:45 - 3:45 p.m.	Panel 5	Insurance and Assurance	Moderated by: Emily Frye, GMU
	1	Known Unknowns: The Delusion of Terrorism Insurance	Michelle Boardman, GMU
	2	Assuring the Energy Grid	Anne Dailey
	3	Should Vulnerability Be Actionable? Improving Critical Infrastructure Computer Security with Trade Practices Law	Jane Winn, UW
3:45 - 4:00 p.m.	Break		
4:00 - 4:45 p.m.	Panel 6	Civil Rights	Moderated by: Ken Newbold, JMU
	1	War in Peace. Preserving the Rights to Strike, Lockout, and Replace in the Age of Terror	Ross Davies, JMU
	2	Probabilistic Analysis of Privacy Risks: Proposal for a national database of incidence of privacy violations	Farrokh Alemi, GMU
	3	Political Ignorance in the War on Terror	Ilya Somin, GMU
5:30 - 7:00 p.m.	Reception		
7:00 - 8:00 p.m.	Dinner	Keynote Address	Steven Simon, Senior CIPP Fellow, Rand
Friday, October 1			
8:30 - 9:00 a.m.	Breakfast		
9:00 - 10:00 a.m.	Panel 7	Regional and International Issues	Moderated by: Emily Frye, GMU
	1	International CIP Program	Randy Jackson, GMU
	2	Port Security	Willem Holleman, GMU
	3	Economics, Security and the Logistics of the Shopping Mall	Marc Thibault, GMU
	4	Disaster Resistant Communities	Roger Stough, GMU

Friday, October 1 (Continued)			
10:00 - 10:45 a.m.	Panel 8	Biodefense	Moderated by: Christine Pommerening, GMU
	1	Protecting the Nation's Blood Supply	Arnauld Nicogossian, GMU
	2	Preliminary Report: Development of Recombinant Biological Vaccines and Critical Diagnostics to Address the Threat of Bioterrorism	Ronald Raab, JMU
	3	Development of an Indoor Air Quality Sensing and Alert/Alarm System	Gene Tucker, JMU
10:45 - 11:00 a.m.	Break		
11:00 - 12:00 p.m.	Panel 9	Cooperation and Coordination	Moderated by: Rod Nydam, GMU
	1	Building an Undergraduate Security Curriculum	Anne Marchant, GMU
	2	Getting a Grip on Strategic Alliances	Ken Newbold, JMU
	3	Network Responses to Network Threats: The Evolution Into Private Cyber-Security Associations	Amitai Aviram
	4	A Cybersecurity Symposium: An Opportunity for Collaboration for Researchers, Security Officers and Funding Agencies	Joy Hughes, GMU
12:00 - 1:00 p.m.	Panel 10	Social and Organizational Aspects	Moderated by: Ken Newbold, JMU
	1	Critical Infrastructure Protection Oral History Project	Rebecca Luria, GMU
	2	Contribution of Organization Studies to Critical Infrastructure Protection	Todd La Porte, GMU
	3	Emergent Best Practices for Collaborative Partnerships in Infrastructure Protection	Sandra Cheldelin, GMU
	4	Comforts of Home: Humans as a Critical Infrastructure	Stephen Stewart, JMU
1:00 - 1:30 p.m.	Lunch	Closing Remarks	Dean Daniel Polsby, GMU
1:30 p.m.	Adjourn		

Remarks of Daniel D. Polsby

Acting Dean, School of Law, George Mason University



Although I have been with the law school for a good while now, I have not been involved with the substance of CIP Program grants before, and I found this year's proceedings most educational.

May I bring, with the eyes of an outsider, a basic question to these proceedings? We seem to be very good at asking cost - benefit questions when it comes to particular microcosms - the blood supply, the H-VAC systems of buildings, shopping centers and of course many, many others. But from an economic point of view, the true "cost" of anything is not the sticker price, but rather, the lost opportunities of investing a given amount of cash, brainpower and effort in some alternative use. If we sum up the costs of robusting the many microcosms that we are studying - of increasing the hardness and survivability and smartness of systems as they confront the spectrum of mischief that may be aimed at them - how much money and sweat equity, and how much diversion of resources into these activities - are we really talking about? I can't answer that question and it dawns on me that none of you can answer it either, but I am thinking the number might be pretty intimidating before we have accounted for all the factors that should be added in.

The way I think about this problem with my novice's head is to use as a model our own building, the GMU Law School building, or Arlington One as it is called inside the university. I take this as my model because a number of you have seen the building and can easily visualize what I am talking about. Arlington One, for those who don't know it, is a four story building that is sited near the intersection of two busy urban streets. It is surrounded by taller buildings with clear sight lines to any of the windows and porches of our building. There are five exit points in the building, two people entrances, a loading dock and two entrances to parking decks located inside the building. We have an H-VAC system that forces air through the entire physical plant. There is an adjacent parking lot -- and lots of other stuff, but let's stop here. How would I protect this facility from a truck bomb, a sniper, a suicide bomber, someone introducing a toxin or pathogen into the ventilation system? The building wasn't built with these threats in mind. We could retrofit it to reduce all of these risks, of course, but these are hardly the only risks we would have to worry about, only some of the most obvious. We can rely on a mischief maker to find the weakest link and exploit it. Were we to hire a security consultant to fix our building, I am reasonably sure that, after some back of the envelope calculation, he would tell us - just tear the building down and start over, designing from the beginning with your security objectives in mind.

Have we set for ourselves, in effect, the task of strengthening 40 or 50 or 100 links in a chain that may be 200,000 links long?

Does that model tell us anything about the country, or the world, as a whole? Have we set for ourselves, in effect, the task of strengthening 40 or 50 or 100 links in a chain that may be 200,000 links long? I ask this question with the background of a criminal law teacher, which is what I used to be, because in criminal law generally we encounter questions that are strikingly similar. We deal with a mix of risk and uncertainty where uncertainty predominates. Mischief makers think, they can overcome specific barriers that are put in their way, they can substitute away from difficult mischief to easy mischief. We can and should take a variety of cheap *(Continued, Page 16)*

Thoughts on the CIP Program Offsite Workshop

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

The reports of researchers at the recent CIPP offsite were truly impressive. The offsite offered a unique opportunity for fellow researchers to share quality work cutting across a wide breadth of areas that one would not get in traditional disciplinary oriented conferences or workshops. I am confident that once again, new connections among researchers were made that will benefit our work in CIPP and benefit the individual researchers.

While we have achieved many noteworthy accomplishments through the work of CIPP supported researchers, two of the more significant accomplishments, from an administrative and systems perspective, have been our demonstration that effective partnerships among institutions of higher education can work and how each of our respective institutions has leveraged our CIPP support and activities to build even greater interdisciplinary collaborative efforts on our campuses. At James Madison University, we have incorporated our CIPP work with other homeland security research, academic program and outreach efforts under the umbrella of the Institute for Infrastructure and Information Assurance (IIIA). Consistent with our goals and values in CIPP, efforts under IIIA include applied research, where we have faculty from every academic college within the University involved as well as faculty from sister institutions, and academic program and curriculum development which again cuts across the traditional college boundaries. The interdisciplinary and complex critical infrastructure protection issues are both well-suited to and require such a cross/interdisciplinary approach. Thus, CIPP has been a good stimulus for positive change within the institution.

Christopher T. Hill, Vice Provost for Research and Professor of Public Policy and Technology, George Mason University

It is often said that "success has many fathers," and at the recent CIPP Offsite, I was very pleased to be one of the many fathers, or at least one of the many godfathers, of the George Mason/James Madison Critical Infrastructure Protection Program. This very successful offsite was noticeably different from the first one held a year ago at the same place-the beautiful Airlie House retreat near Warrenton, Virginia.

At the end of the first year, CIPP had started a number of new projects, not only in the two central universities but also in a number of other universities and institutions. Most of the presentations a year ago were about ideas and promises, but few were about accomplishments, findings, conclusions or recommendations for action. In addition, many of the CIPP investigators met each other for the first time at the 2003 offsite, and there was much jostling for advantage, but not much seeking for common ground or new alliances.

Things couldn't have been more different this year. A number of projects have yielded tangible results. Others reported discovering new connections or talked about fresh insights into old problems. Many of the papers and presentations were quite thought provoking. Cross-institutional teams reported, and there was a lot of interchange between researchers across institutional boundaries, *(Continued, Page 11)*

Hill *(Cont. from Page 10)* not only in question and answer sessions, but also in the hallways, during breaks, at meals, and "after hours." My only regret is that the organizers shoehorned so many folks into the program that there wasn't enough time for discussion or further exploration of some of the stimulating work that was presented.

The offsite demonstrated that the CIPP teams at Mason and Madison have begun to coalesce into a single large well-functioning machine. To be sure, they have distinct institutional styles, and work remains to be done to smooth off some rough edges here and there. Both teams need to work at highlighting and promoting the increasingly visible and valuable "CIP Program" identity, while respecting the needs each has to firmly establish its place in the ranks of outstanding universities in the "critical infrastructure protection space."

In a very stimulating closing address, Prof. Dan Polsby, Acting Dean of the George Mason University School of Law, challenged everyone involved in the CIP Project to consider whether deterrence has been given sufficient weight as a strategy for coping with the challenges of protecting critical infrastructures against foreign and domestic assault. Just as communities can never become "safe enough" only by erecting ever higher walls to keep the threat of crime at bay, so it may be, he suggests, that our nation cannot hope to make itself as safe as it wants to be only by building ever more protections into our ports, airports, networks, vulnerable commercial structures, government buildings and the like. Speaking, in his own words, as "an old criminal lawyer," Polsby urged that we pay more attention to deterrence, along with the work we do on detection, prevention, response, and reconstruction as *(Continued, Page 16)*

Dr. John B. Noftsinger, Jr., Associate Vice President and Executive Director, James Madison University

After attending the Critical Infrastructure Protection Program Off-Site Meeting, it was clear to me the immense progress the CIP Program has achieved over the past two years. The quality of research is intellectually stimulating and the faculty and students participating should be commended for their dedication to furthering the nation's security. I am most impressed with the collegial, collaborative and interdisciplinary nature of the ongoing CIP Program efforts which was evident throughout the two days at Airlie. It is also encouraging to hear of the number of doctoral, graduate, and undergraduate students who have been given the opportunity to participate in the cutting edge research underway at both universities. One strength of the CIP Program is the commitment to providing unique learning opportunities to our students.

In my remarks, I commented that the opportunity to participate on this important project has been exciting, rewarding, and career changing for me and my faculty colleagues that have also engaged. I have been extremely pleased with the ability of James Madison and George Mason Universities to work closely and collaboratively in developing such a successful program. Throughout my career in higher education, I have worked to develop partnerships and alliances. Through the collective effort of both universities and their desire to advance the relationship, the CIP Program has been a success as well as professionally rewarding. You might say the CIP Program "is our finest moment." As executive director of JMU's Institute for Infrastructure and Information Assurance, I have been able to work closely with a number of talented, dedicated, and committed faculty and students. I truly value the personal and professional relationships that have been developed with colleagues at George Mason and look forward to *(Continued, Page 16)*

What Drives Islamist Violence?

Part 1 of 2

Steve Simon
Senior CIPP Fellow, RAND Corporation

The global jihad against the United States and its allies is fueled by many factors. Some of these are systemic, some contingent. But the fact there are so many sources of this violent impulse means that no one policy is going to counter it. The contributing factors stem from sociological, political, economic and operational developments. In this issue, we look at some of the social and religious developments. Next month, we will explore political and tactical trends.

Perhaps the most important sociological factor is the globalization of Muslim identity. Although Muslims have always been urged to self-identify as part of a broader *umma* (the community of all Muslims), in practice, other competing loyalties based on ethnicity, nationality, tribal group, economic class have exerted powerful influences of their own. Today, globalization has helped fuel a revival of a Muslim identity in which North Africans are increasingly likely to identify with the struggles of their co-religionists in Central Asia and European Muslims with conflicts in the Middle East. Other key sociological elements include the proliferation of informal networks that continue to expand in the Muslim World in response to government repression, inefficiency, corruption, or a mix thereof. This arena of unlicensed activity has given jihadist groups a ready made system for the movement of money, people, weapons, and of course ideas.

The realm of ideas, moreover, is now up-for-grabs as the authority of establishment clerics, who might be inclined to counsel their flock toward moderation, has been broken. How? As literacy has spread more Muslims could interpret the scripture for themselves. At the same time, mainstream clerics were tainted by their dependence on repressive governments. As a result, the traditional "brake" on runaway interpretation of sacred texts no longer has stopping power. This said, the practice of Islam is still primarily reflexive and strongly tied to ritual for most believers, but the democratizing effect of education has given those with a political agenda a powerful tool - religion - to pursue their goals. These changes have been accelerated by powerful media in the form of the Internet, satellite television, and the venerable audio and videocassette. The weakened position of liberal reformers in the Muslim World has allowed Islamists to corner the market on opposition to status quo politics. In the past, pluralistic secular-oriented reformers could check the popularity of Islamists. Most have now lost influence, however, discredited by their association with nationalism and socialism, both derided as Western, inauthentic, imports.

Islamist influence has ridden the shock waves of powerful, inflammatory images. The killing of Mohammed al-Durra - the child shot in Gaza during the intifada - or American bombing of targets in Afghanistan, and Israeli tanks rolling through Palestinian towns are frequently presented in a decontextualized fashion intended to depict the roles of villain and victim in an easily digestible format. This raw footage makes its way into Arab pop music videos, pan-Arab news coverage and websites, where it is used to justify violence and rally people to the cause of Islamic faith under attack.

To be continued in the November issue of *The CIP Report*. ❖

Preparedness, Evacuation, Shelter: Collaborating to Develop Solutions Within Emergency Planning in the Shenandoah Valley

Joshua Barnes
Institute for Infrastructure and Information Assurance, James Madison University

The CIP Program has funded research at 15 universities, engaging 70 researchers, with 200 students involved. This article highlights some of the student research that is taking place through CIP Program funding.

The Institute for Infrastructure and Information Assurance (IIIA) has been actively working to develop concepts that will eventually be brought into practice for the Shenandoah Valley. This work has been divided into two primary areas. The first is in developing a decision support matrix that will be useful for the first responder community in dealing with weapons of mass destruction incidents. The matrix defines all of the potential weapons of mass destruction in the B-NICE (Biological, Nuclear, Incendiary, Chemical, and Explosive) categories. Once first responders define an event based on the matrix, complementary pages indicate the basic actions that must be exercised by public health, incident command, security, and fire/hazmat officials. A second part of this matrix outlines historical examples of events that would fit into the possible categories for a weapon of mass destruction (WMD). The WMD threat to the Valley is very real. Staunton, for example, could be one of many sites of a smallpox outbreak. Because the Valley is vulnerable, the matrix will be useful in guiding the actions of the first responder community in mitigating the disaster.

The second area that the IIIA is exploring is in creating Homes Away from Home. A Home Away from Home is an emergency shelter that has been planned to provide recreational and entertainment attributes that will support the psychological needs of disaster survivors. Imagine how much better it would be to know that a shelter will have a television with a VCR so you can bring your child's favorite movie. Eventually, a Geographical Information System will be created to identify all of the available shelters in the region, and then identify which communities are served by which shelters. IIIA hopes to eventually cooperate with the major utilities to distribute information on the household level about their closest shelters.

Threats to homeland security can come in forms other than terrorism. Any disaster that impacts your way of life is a threat to our security. Because of these threats, the Institute for Infrastructure and Information Assurance is actively pursuing grants and research opportunities to help ensure the security and responsive capabilities of everyone in the Valley.

Another avenue that IIIA is taking in improving security in the Valley is through work with the Central Shenandoah Planning District Commission (CSPDC). The CSPDC is a regional commission composed of twenty-one local government jurisdictions from the town to the county level. The role of this CSPDC in the Shenandoah Valley is to promote cooperative approaches to land use planning, flood mitigation, economic development, and transportation issues to name a few. IIIA and the CSPDC have reached out to promote initial research results to local governments and first responders. The Decision Matrix has already been distributed to several emergency managers in the region through the CSPDC. Also, IIIA hopes to provide assistance to the town of Bergton,VA, with its emergency sheltering needs. As IIIA is an applied research organization, the opportunity to work with the Central Shenandoah Planning District Commission is an excellent opportunity to reach the individuals our research is designed to help. ❖

RTOs: Improving the Reliability and Security of the Transmission Grid

by Edward L. Flippen*

Electric utility deregulation, which started out as a movement to improve reliability and reduce prices, was almost ended by the California fiasco, the bankruptcy of Enron, and the worst blackout in US history. Indeed, the actions taken by many states following these and other events demonstrated a resolve to halt deregulation and, in several instances, turn the clock back to the "good old days" of "cost-plus" regulation.

We all remember those "good old days." Utilities built whatever type and size facilities they wanted; ratepayers paid for managements' decisions, good or bad; and rate cases were filed every couple of years to cover continually increasing costs. Simply put, in the "good old days" customers got all the risk, and management, regulators, consultants, and lawyers got all the rewards. It is no wonder that the good old days look so good to so many.

In some states the good old days remain, but in others there is no going back. The genie is out of the bottle. Management has changed, thousands of employees have been let go, "build" decisions are based on sound capital budgeting analyses, and utilities are joining regional markets to improve reliability and reduce cost. That said, the new economic order is not pretty. Competition never is. Companies struggle, customers are taken advantage of by "fly-by-night" marketers, alternatives can be confusing, and customers have to make choices. These are the by-products of competition, but so are recruiting and maintaining the best and brightest managers, reducing costs, improving efficiencies, quantum leaps in technology, and perhaps most important, conservation and a better environment.

True, competition has been a scary road to date. California's deregulation plan looked stupid (and much of it was). Enron demonstrated how major changes in an industry structure create opportunities for the wheeler-dealer. And the August 14, 2003, northeast blackout - the worst in US history - points out how vulnerable our safety, health and economy are to disruptions in electric service. All of this causes us to question the need to change from the "good old days" of regulation to the "new days" of deregulation. Worse yet, the cases of California, Enron, and the blackout do not end our questions; they have only begun. Many other events will cause us to question whether deregulation of electricity, a service as fundamental to our economic well being as air and water, will improve electric efficiency and reliability, lower prices, and create a better environment. Most importantly, it has awakened us to the need to improve the reliability and security of the transmission grid.

According to the North American Electric Reliability Council (NERC), "North American transmission systems are expected to perform reliably in the near term...[but] portions of these systems are reaching their reliability limits."[1] Of course, that is understandable. The extraordinary increase in power transfers between utilities together with a recent decline in the level of transmission investment is presenting a significant challenge to policy makers, regulators, and electric utilities alike.

The simple answer is to increase the capacity of the system and/or locate new generation near load centers. Needless to say, while the answer is simple the execution is anything but simple. Anyone who has ever worked on *(Continued, Page 15)*

** Edward L.. Flippen is a partner with McGuireWoods LLP, lecturer in law at the University of Virginia School of Law, and Distinguished Senior CIPP Fellow at the George Mason University School of Law.*

RTO's *(Cont. from Page 14)* locating a transmission line or power plant near a population center knows the difficulty - it is often nearly impossible. Regardless of the issue, the transmission system must be upgraded and expanded and new generation is required in both the short- and long-term. Electric utilities continuously wrestle with the regulatory, public, political, and financial quagmire that erupts when they are building new transmission and generation facilities. Luckily, there is a short-term solution that will improve electric reliability without negatively impacting the public, namely, "managing reliability on a regional basis."

Historically (i.e., before the 1960s) the transmission system was built to serve the loads of individual electric utilities. The construction of the interconnected network of extra high voltage transmission lines in place today occurred between the 1960s and the 1980s.[2] The interconnected network provides some increased reliability and a reduced need for new transmission facilities, but it does not optimize the planning, construction, and operation of electric utility systems. Simply put, on a real-time basis, the control room operator of a local utility does not have the "big picture" of available transmission and generation resources of regional utilities.

The competition movement in the 1990s has fostered the development of new regional transmission entities and the expansion of existing entities such as PJM Interconnection, LLC. What extra high voltage interconnection did to reliability in the 1960s to 1990s, regional transmission operators (RTOs) or independent system operators (ISOs) can do to reliability in the 2000s. In a heavily interconnected system, a strong regional system operator may not be able to prevent individual plant blackouts caused by terrorists or equipment failures, but it can prevent those events from cascading any further. The regional system operator is not operating solo. He or she sees what problems are occurring throughout the region and, most importantly, knows what resources are available throughout the region to address those problems.

The interconnected network provides some increased reliability and a reduced need for new transmission facilities, but it does not optimize the planning, construction, and operation of electric utility systems.

This is not to suggest that requiring electric utilities to join RTOs is the only solution to reliability. Utilities still must build generation plants and establish transmission lines to serve their growing number of customers, and RTOs have no "silver bullet" for the "not in my backyard" objections to such projects. And the shared jurisdiction of federal and state regulators over transmission facilities and operations further complicates the planning and construction of these facilities. Regardless, the regional oversight of our electric transmission grid should be a "no brainer" and, in fact, probably is. Where the rubber hits the road, so to speak, is how much authority the RTOs will have over planning, construction, and operation. An RTO must be more than just a central coordinator for the local utilities; the RTO must have clear responsibility, authority, and ability to take whatever action is needed in a particular circumstance. The RTO operator cannot prevent equipment failures, but he or she should be better able than an individual control room operator to isolate a particular problem within a given region. Whatever the tensions associated with shared federal and state responsibility of transmission facilities and operation, there should be no disagreement about RTO membership enhancing the reliability and security of the 160,000 miles of electric transmission grid. ❖

[1]North American Electric Reliability Council, *2003 Long-Term Reliability Assessment: The Reliability of Bulk Electric Systems in North America*, at 5.
[2]*2003 Long-Term Reliability Assessment*, at 43.

Hill *(Cont. from Page 11)* we seek ways to make our nation safer.

I'd like to close by noting the excellent job that Emily Frye, Associate Director of CIPP, and Dr. Christine Pommerening, CIPP Post-doctoral fellow, did in organizing and running the CIPP offsite. CIPP's able Director, John McCarthy, could not participate in this year's offsite owing to his need to rest and recover from major surgery. While he was very much missed throughout the event and we look forward to his imminent return to the helm, his colleagues did a most credible job of stepping into the breech.

Noftsinger *(Cont. from Page 11)* continuing to expand the connections between our two universities.

While the CIP Program has accomplished a great deal in a relatively short amount of time, we must not lose focus on our efforts to help provide solutions to the issues facing the nation's critical infrastructure systems. I challenge my colleagues in higher education to continue to work together with other academic institutions, to partner with businesses and government agencies and bridge the gap between physical and cyber security and the scientific, legal and business worlds. Research in critical infrastructure protection is high on the national agenda and the CIP Program must strive to continue its leadership in this area. We in education must not forget that we need to train and educate the future owners and operators of infrastructure systems as well as provide research based solutions. I was pleased to hear at the off-site of the ongoing curriculum development projects and encourage faculty to explore new ways in which teaching and learning can occur.

I look forward to the future accomplishments and the growth of the CIP Program.

Polsby *(Cont. from Page 9)* precautions to defeat half-headed mischief makers - locks on doors and so on - but the reality is that using this sort of particularistic device against someone whose ambition is not particularistic but global - namely to do us harm by inflicting costs on us - is apt, in the end to disappoint us. The criminal law aims to cure the problem in a different way - by changing the incentives of malign actors with punishment: it tries to put a price on misconduct in order to deter it.

Deterrence seems to be missing from our conversations here. It shouldn't be. Deterrence is in many cases far cheaper than precaution-taking. We have a policeman in Arlington One - the capital equivalent of about $5 million or so - in lieu of lots of other, more passive security precautions that would, counting information costs, surely turn out to be more expensive.

We must leave it for another day to explore whether greater investments in deterrence might be more nearly optimal than piecemeal defensive actions in the form of gizmos and reworking politico/administrative structures, could possibly be - but if my thought experiment with Arlington One is of any use at all - and I freely confess it may not be - the implication is clear. There is in the last analysis, no way to defend against a resolute mischief maker. He has to be discouraged. Figuring out how to do that, and doing it, is likely to be cheapest way to go. ❖

Overview *(Cont. from Page 5)* a particular symposium that brought together cyber-security experts, thus offering a forum for structured collaboration between researchers, security officers, and funding agencies.

Social and Organizational Aspects

Panel ten emphasized the underlying social and organizational aspects of critical infrastructures and their protection. Moderator Ken Newbold first introduced Rebecca Luria and Kathi Ann Brown, who jointly reported on the almost completed Critical Infrastructure Protection Oral History Project. Using interviews and archival research, this project tracks and documents the institutional evolution of CIP beginning in the 1990s as seen by the actors originally involved in it. The importance of the people behind the scenes was also one of the central arguments of Todd La Port's comprehensive discussion of critical infrastructure operations and operators. The particular contribution of organization studies to CIP is the recognition of so-called high reliability professionals, and how their socialization, value system, and communication style impact performance in routine and extreme situations. Sandra Cheldelin then sketched out ongoing research into how best practices can be identified to foster partnerships between representatives of competitive industries for more effective collaboration in CIP. The final presentation of this offsite workshop was, fittingly, about the 'Comforts of Home', referring to how humans react to hazards and disasters. Benjamin Delp and Joshua Barnes described a planning approach for risk communication and shelter-in-place that takes this into account.

Outlook

The closing thoughts by Dan Polsby, Acting Dean of the GMU School of Law, centered around the need for looking above and beyond protecting structures. A criminal law perspective, for example, would consider the potential for and cost-effectiveness of deterrence [see separate article in this newsletter].

Continuing the tradition started last year, a book was produced based on the workshop contributions. This second volume of CIPP working papers contains project reports, research overviews, and initial findings from a variety of academic disciplines. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructures. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Program. 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.