MARCH 2004 / VOLUME 2, NUMBER 9

THE CIP REPORT

Higher Education

Role of Universities in Preparing Professionals 2
Building an Undergraduate Security Curriculum 3
Target Washington 4
Legal Insights 5
EDUCAUSE 7
Cyber Security Symposium . . .8
REN-ISAC 10
ORAU Advisory Team 11
VA SCAN 12
NSA Centers of Academic Excellence 13
CIIP Handbook Event 16
Security in Wireless P2P . . .17
Homeland Security Centers of Excellence 18

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*

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

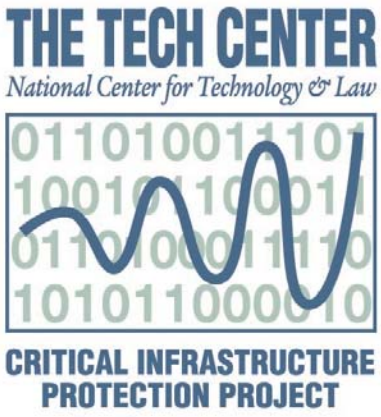
Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

Contact: cipp01@gmu.edu
703.993.4840

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

Although the system of Higher Education is not a critical infrastructure in itself, it has a significant role to play in critical infrastructure protection. The nation's colleges and universities contribute to CIP in three central ways. First, they educate and train tomorrow's CIP workforce-not simply as information security professionals, but as practitioners who understand the multifaceted approach required for securing the nation's critical infrastructure. Universities also promote public awareness of the issues surrounding homeland security and its CIP components.

Second, universities play a key role in research and development. From basic ground-breaking activities like developing new methods for secure computing, to applied research activities such as providing a forum for facilitation and cooperation to develop new government policies or business practices.



Finally, universities' open environment to afford academic freedom presents unique security challenges which include: protecting sensitive information and products developed through research; building a secure environment for a diverse constituency that includes students, faculty, and administration; and, mitigating their own cyber and physical threats.

This issue of *The CIP Report* focuses on Higher Education's complex role in critical infrastructure protection, and introduces our readers to some of the initiatives taking place in education, research and development, and security. Ongoing work in the development of undergraduate security curricula and preparing the next generation of infrastructure professionals is highlighted. An example of academic collaboration to address cyber security research challenges is captured in the article about the Southeastern Universities Research Association (SURA) Symposium, held at GMU under the leadership of Dr. Joyce Hughes, GMU's Vice President for Information Security.

We also include thoughts from leaders in the field of CIP from industry and academia as a means of sharing opinions on higher education's role in critical infrastructure protection, as well as introducing some of the names and faces active in this vibrant and pressing national security arena.

As an example of the vibrancy of academia in the area of CIP and homeland security, a televised town hall meeting addressing the specific threats faced by the National Capital Region was held at George Mason University in late February. We have included an article on this exciting event, Target Washington, which was hosted by Frank Sesno and included an impressive panel of speakers, most notably Secretary of Homeland Security Tom Ridge.

We hope that you continue to find *The CIP Report* an informative newsletter and that the information contained in this issue helps to draw a picture of the extensive role higher education plays as both a key player and as an honest broker in critical infrastructure protection.

The Role of Universities in Preparing The Next Generation of Infrastructure Professionals

George H. Baker, Ph.D.

Institute for Infrastructure and Information Assurance

James Madison University

Highly efficient, complex, and interdependent infrastructure systems including electric power, telecommunications, transportation, water utilities, food distribution, housing and shelter, public health, finance and banking are foundations of modern societies. Over the last 3 years, the United States has become acutely aware of the importance of civil infrastructures and their criticality to the nation's economy and quality of life. Our reliance on these systems makes them especially attractive targets for attack. Both cyber and physical attacks are known to cause major disruptions of the sometimes-fragile systems. The incidence and cost of natural disasters has also increased in recent years. The systems are so complex that we still have much to learn about their failure modes and the cascading effects caused by their elaborate interdependencies. Failure consequences can be extremely severe. Exercises simulating major infrastructure disruptions point to consequences ranging from widespread loss of critical services to the breakdown of national governance.

Universities need to play a central role in infrastructure assurance but have not yet realized their full potential. To date, we have done a good job of addressing cyber security as evidenced by the large number of world-class information security centers and degree programs producing competent information security professionals. There are now more than 50 national centers of excellence in information security education.[1] Information security degree programs, both resident and on-line, are available at many of these institutions through the Ph.D. level. Universities are also involved in real-time assistance vis-à-vis cyber incidents with operating emergency response centers at several universities (Carnegie Mellon, USMA, Indiana, and Wisconsin as examples).

There is no doubt that cyber security is important because of the ubiquitous nature of our information networks, providing the nervous system pathways within and among most critical infrastructures. However, we need to come to grips with the challenges posed by the larger problem set of infrastructure assurance. Cyber security is an important part of the equation, albeit a subset. A balanced approach to infrastructure assurance is needed in addressing physical and cyber concerns.

R.G. Little, Director of the National Research Council Board on Infrastructure contends that existing infrastructure managers must routinely synthesize information from a broad range of disciplines including civil engineering, materials science, government operations, economics and finance, social and political science, and environmental science. Civil engineers are competent to deal with the technical/physical aspects of infrastructure issues but aren't trained in relating technical issues in complex public forums. Public administrators in most cases lack the technical background needed to evaluate technical solutions to public needs. The challenge is the sheer complexity of infrastructure from technical, financial, and socio-political standpoints and the multidisciplinary skills

(Continued, Page 15)

Building an Undergraduate Security Curriculum

Anne Marchant, Edgar H. Sibley, Hugh Tazewell (Taz) Daughtrey Jr.
George Mason University and James Madison University

George Mason University (GMU) and James Madison University (JMU) were funded jointly under a CIPP grant to develop and implement the curriculum of a cyber-defense undergraduate program over a 15 month period through the fall semester of 2004. Course material is now being developed and incorporated into two BS programs: in Computer Science at JMU and in Information Technology at GMU. The curriculum includes coursework in programming, operating systems, and networking as a basis for the major courses in security, which include security technology, forensics and auditing, network security and intrusion detection, risk management, policy, modeling, and authentication. Modules in ethics and social responsibility are woven throughout the courses.

The first major output will occur in the 2004 summer semester: a prototype capstone course for a select group of undergraduate students with a few special graduate students at GMU's Prince William (PW) Campus. This is designed to be similar to the final course at the military service academies; i.e., it culminates in a war-game that involves cyber-attack and defense. JMU faculty and a teaching associate will staff this effort, In the fall semester, the curriculum will be expanded to JMU and culminate in attack and defense exercises between JMU and GMU classes over a virtual private network (VPN) - probably in the spring semester of 2005. This course will serve as a tool for assessing the effectiveness of the entire curriculum.

The curriculum for the course is being developed by two research associates (RAs) at GMU in conjunction with Dr. Sibley and with help from faculty now teaching a graduate course at George Washington University, who are also helping in the design of modifications to the current labs on the PW Campus for this new and entirely lab-based course.

Regular offerings of the capstone will start in subsequent terms. A bridging course will be added to provide a way for top undergraduate students to supplement their information security knowledge as an elective or as a rapid start for a Master's degree at GMU in Information Security Assurance; this curriculum need is currently being investigated by one of the RAs.

As a result of the summer exercise, several practical benefits will accrue: the architecture of the laboratories, the curricula, and a description of the problems and successes of the program will be reported widely in papers and talks at conferences. Our intent will be to expand such exercises to conforming state and local universities and state institutions of Virginia. Later we expect to expand this effort and join others in developing such exercises in *(Continued, Page 9)*

Linwood Rose, Ph.D
President
James Madison University

The time has come for leaders in higher education to recognize and creatively respond to the opportunity and realities that protecting the national critical infrastructure provides. In order to effectively do this, it is paramount that the academy embraces and implements a vision that balances basic with applied research and integrates these into the curriculum.

Furthermore, as leaders within our field we must facilitate technology transfer, be truly interdisciplinary in program development and deployment, be engaged through strategic alliances and collaborative efforts, and, as our forefather James Madison would advocate, balance public interest/national security with individual rights.

Premier Show Brings Candid Homeland Security Discussion to GMU

By Frank Sesno

The face of homeland security assumed a regional profile on February 24, when more than 300 people gathered in Harris Theater at George Mason University to attend a town hall meeting focusing on the special threats and challenges confronting the National Capital Region (NCR). Secretary of Homeland Security Tom Ridge, the Mayor of Washington along with his counterparts from neighboring Fairfax County, Virginia and Montgomery County, Maryland came together with other local decision makers, first responders and public health officials for an unprecedented discussion that cut across regional and disciplinary boundaries. The discussion touched on issues ranging from evacuation and the lack of backup power for traffic lights to surge capacity in the region's hospitals and the allocation of resources. The program, *Target Washington*, was broadcast on public television WETA in Washington and drew considerable national and local press attention.

What we heard in 90 minutes of conversation was both impressive and daunting. Impressive because it was clear that a great deal of coordination work around communication and decision making has already taken place across jurisdictions and agencies that represent the NCR.

Daunting by virtue of the sheer scope of the task, the nature of the threat and the number of people and places involved. Secretary Ridge framed the discussion with a disarmingly simple observation: "We are the nation's capital. We have been subject to an attack before."

TARGET WASHINGTON

We began the panel discussion with a hypothetical scenario: a surge of sick people displaying similar conditions begin arriving at Fairfax County hospitals. I asked the county's Director of Health, Dr. Gloria Addo-Ayensu, what she would do first. She said she would contact the regional epidemiologist to determine if the symptoms were showing up elsewhere around the region. Within minutes, hospitals, public health experts, local law enforcement, emergency management, elected leaders, and homeland security officials would be talking among one another in addition to conference calls to assess developments and monitor the unfolding situation. County, state and federal jurisdictions would be placed on alert. Even before any formal public notice, it's likely the media would report what was happening, putting even more pressure on officials scrambling to determine if the illnesses were coincidence or bioterrorism.

The scenario demonstrated how fast information moves and how little time officials have to react - one of the toughest challenges in homeland security.

The scenario led to a discussion that demonstrated the unique and immensely difficult reality of the NCR. While coordination among the various jurisdictions and agencies across federal, state, city, and county lines has made great progress since 9/11, it is nowhere near complete and some glaring weaknesses

(Continued, Page 14)

LEGAL INSIGHTS

by Emily Frye

HOMELAND SECURITY'S CHANGING LIABILITY REGIMES

By Guest Columnist Steven E. Roberts

When United States District Court Judge Alvin Hellerstein refused to release Boeing Corporation from liability in the September 11 terrorist attacks, he held that "...it was reasonably foreseeable that a failure to design a secure cockpit could contribute to a breaking and entering into, and take-over of, a cockpit by hijackers or other unauthorized individuals...."[1] Yet, this preliminary ruling has significance far beyond the individual defendants whose September 11 liability is now in the hands of the courts. For the nation's critical infrastructure sectors, the ruling signals a possible paradigm shift in the legal liabilities associated with terrorism. Critical infrastructure owners and operators may be held liable for damages based upon a duty to prevent or mitigate acts of terror.

On the afternoon of August 14, 2003, approximately 50 million people in eight states and the Canadian provenance of Ontario lost electrical power. President Bush and then Canadian Prime Minister Jean Chrétien quickly established a U.S.- Canadian Power System Outage Task Force to investigate the cause of the massive, cascading power failure. Among other findings, investigators discovered that several parties, including FirstEnergy Corporation, violated North American Electric Reliability Council (NERC) standards for safe and reliable power grid operations. While NERC has since ordered those responsible for the power outage to take corrective action, the case of FirstEnergy begs an important question: had the cause of the power outage been a deliberate act of terrorism, could damaged parties hold FirstEnergy and others liable for failing to prevent a terror-induced blackout using Judge Hellerstein's expansive view of "reasonable forseeability?" Maybe so.

It is arguable that terrorists will target power plants and other critical infrastructures. Several considerations support this proposition. First, Osama bin Laden has publicly lauded the economic harm caused by the September 11 attacks.[2] Considering that al Qaeda's version of asymmetric warfare blends physical loss with economic loss, an assault against a power plant or other high value critical infrastructure to cause economic harm comports with al Qaeda's *modus operandi*. This is particularly true if the results of the attack cascade into other critical infrastructure sectors, thereby increasing the economic repercussions.

Second, it is now known that al Qaeda's focus on critical infrastructures is real. Operatives used the Internet to conduct reconnaissance of critical infrastructure sites, including communications networks, water storage and distribution facilities, and natural gas facilities. They even showed interest in Supervisory Control and Data Acquisition systems used to control many critical *(Continued, Page 6)*

Alan Merten, Ph.D
President, George Mason University

Higher education has never been more prepared to shoulder the weight of responsibility required to secure and protect our critical infrastructures. Each university brings unique capabilities and expertise based on the talents of dedicated faculty and staff, and the promise of new generations of emerging students. These are enhanced and strengthened through the partnerships and collaboration that is possible.

The issues facing our critical infrastructures are complex, interwoven and highly interdisciplinary in nature. The response to these threats must be equally strategic and complex, joining universities with private and public entities in a new approach to partnerships. Only partnerships united in mission and built upon trust relationships between leaders within higher education, private industry and government agencies will enable us to move toward the more secure future we desire.

Legal Insights *(Cont. from Page 5)*

infrastructure components.[3] More alarming, terrorist interest in critical infrastructures has moved from theory to practice: in October 2003 Iyman Faris, a confessed al Qaeda operative living in Ohio, received a 20 year prison term for providing material support to al Qaeda. Faris supported a failed terror plot to destroy a New York City bridge and derail trains.[4]

Finally, the January 2004 attack on a power plant in the Philippines by rebels armed with machine guns and grenade launchers demonstrates that terrorists understand the vulnerability of soft critical infrastructure targets. While this attack seems of little consequence in the United States, it may be a harbinger of things to come, especially considering the reported links between the Filipino terror organization Abu Sayyaf and al Qaeda.

Consequently, at least as a matter of tort theory, it is reasonably foreseeable that critical infrastructures will be the focus of future terror plots. Given this risk and the continued threat of terrorism more broadly, critical infrastructure owners and operators who fail to implement security measures may be held liable for ignoring a "...recognizable danger, based upon knowledge of the existing facts, and some reasonable belief that harm may possibly follow."[5] Ironically, the cost to defend such lawsuits would almost certainly exceed the cost of implementing security measures in the first place.

This is not to suggest that the law itself has failed to impose new liabilities in the realm of homeland security. A recent Nevada law mandates that "each resort hotel shall adopt and maintain an emergency response plan."[6] In creating such a law, Nevada recognized its venue as a possible terror target and, in doing so, codified the importance of emergency preparedness in light of terror considerations. Parties injured in a hotel terror attack may now have a specific "homeland security legal claim" upon which to base liability and compel damages. This assumes, of course, that the defendant resort hotel failed to comply with the defined provisions of the statute.

Congress is following Nevada's lead. S.994, the proposed Chemical Facilities Security Act of 2003, would require statutorily defined chemical facilities to conduct vulnerability assessments and implement site security plans.[7] Thus, S.994 would create a clear "security duty of care" for the chemical sector that, heretofore, has been virtually absent. It may be only a matter of time before other critical infrastructure sectors face Congressional action. Under this top down approach, security will no longer be self-imposed and self-regulated by the critical infrastructure owner, but mandated directly by the government.

Legal liabilities in the realm of computer and information security have also emerged. The Health Insurance Portability and Accountability Act (HIPAA)[8] and the Gramm-Leach-Bliley Act (GLBA)[9] impose security requirements for the healthcare and financial services sectors, respectively. Although they neither provide a private cause of action for individuals harmed as a result of non-compliance nor do they relate directly to critical infrastructure protection and homeland security, HIPAA and GLBA are significant: they demonstrate that security can be the basis of sanction and liability. By implication, therefore, critical infrastructure owners and operators would have a hard time asserting that security is not a realistic consideration or drastically outside the standard of reasonable care, given the continued threat of terrorism.

Yet, in the absence of more judicial interpretation, knowing what liabilities may derive from acts of terror is more enlightened supposition than hard legal fact. There can be little doubt that the parties who lose in Judge Hellerstein's courtroom will appeal to the 2nd Circuit Court of Appeals, and then again to the Supreme Court. Then, and only then, will homeland security's changing liability regimes take clearer shape.

[1]Order and Opinion Denying Defendants' Motion to Dismiss at 38, *In Re September 11 Litigation.* S.D.N.Y. (No. 21 MC 97).

[2]Among other Osama bin Laden public statements, see transcript of Osama bin Laden's October 2001 interview.

[3]Gellman, Barton. "Cyber-Attacks by Al Qaeda Feared." *The Washington Post*. 27 June. 2002. See also: U.S. General Accounting Office. *Critical*

(Continued, Page 16)

Information Technology Within the Higher Education Community: The Role of EDUCAUSE

Kenneth Newbold, Institute for Infrastructure and Information Assurance
James Madison University
Allison Burrow, James Madison University

Higher education has faced growing external pressure to utilize technology in the education process. Given the open nature of the academic community, securing electronic data and being responsible users of information technology has conflicted with traditional university norms, over the course of the technology boom of the 1990s, EDUCAUSE has come to the forefront in helping the higher education community address issues and concerns in using and securing information. EDUCAUSE is a nonprofit organization whose mission is to advance higher education by promoting the intelligent use of information technology. EDUCAUSE sponsors programs and various activities which include professional development activities, print and electronic publications, strategic policy initiatives, research, awards for leadership and exemplary practices, and a wealth of online information services. EDUCAUSE wants to help those who lead, manage, and use information resources to shape strategic decisions at every level. While promoting the use of information technology, EDUCAUSE produces three subscription-based programs, EDUCAUSE Center for Applied Research (ECAR), Net@EDU (advanced networking), and National Learning Infrastructure Initiative (NLII) that provide specialized research, opportunities for professional collaboration, and forums for influencing policy.

EDUCAUSE originated from two organizations: Cause and Educom. In 1962, twenty-two directors at colleges and universities organized as an IBM 1401 Users Group at a meeting in Chicago. These individuals represented the first real users of computers for processing administrative data. They called themselves the College and University Systems Exchange (CAUSE). The objective of this original organization was to share information about the new administrative information systems that they were beginning to develop.

Before Cause came to be, in 1964 a group of medical school deans and vice presidents from all over the country came together to found an organization dedicated to the idea that digital computers offered an incredible opportunity for sharing among institutions of higher education. The organization they founded was the Interuniversity Communications Council, Inc., better known as Educom. In 1997 CAUSE approached Educom with the idea of merging the two programs. EDUCAUSE emerged from these two groups and continues to thrive in the new century.

Membership to this organization is open to institutions of higher education, corporations serving the higher education information technology market, and other related associations and organizations. The current membership encompasses nearly 1,900 colleges, universities, and education organizations, which includes more than 180 corporations, and more than 13,000 active member representatives. A broad range of resources and activities are available to all interested employees at EDUCAUSE. This organization tackles a number of policy based issues that affect the campuses of universities across the country. Identity theft, spam and regulation of commercial email, task force on system securities, and file sharing and peer to peer technology are listed as major concerns by EDUCAUSE.

EDUCAUSE hosts five regional conferences and a national conference annually which offer IT professionals, faculty, and university leaders the opportunity to share ideas, discuss best practices, and meet colleagues across academe. Along with these conferences, EDUCAUSE holds leadership institutes, policy seminars, and a variety of other specialized events which are aimed at furthering the issues facing the *(Continued, Page 11)*

SURA/CIPP Cyber Security Symposium

By Maeve Dion

The Southeastern Universities Research Association (SURA) and the Critical Infrastructure Protection Project (CIP Project) sponsored a Cyber Security Symposium on March 8th & 9th, 2004. Representing more than 25 universities and more than twelve states, cyber security researchers and information technology officers met at the George Mason University School of Law to brainstorm solutions to cyber security legal problems.

Joining in this brainstorming effort were David Nelson, Director of the National Coordination Office for Information Technology Research and Development, Carl Landwehr, Director of the Trusted Computing Program at the National Science Foundation, Mark Luker, Vice-President of EDUCAUSE, and Tommy Cabe, Cybersecurity Advisor for the Department of Energy's Office of Energy Assurance.

One key reason for the symposium was to determine the attendees' needs and concerns. Another purpose was to explore collaboration as a tool for developing solutions for cyber security.

The symposium was a great success and generated a specific proposal. The unique characteristics of cyber security often prevent researchers from finding comprehensive security solutions. Instead, such solutions may be better found through layer-specific, problem-solving collaborations between academia and industry, facilitated by independent organizations focused on "the big picture."

The Challenges

Researchers in cyber security face systemic concerns in the rapidity with which new security problems arise, and in the narrowness of cyber security sub-disciplines.

Unlike traditional fields of academic study, the rapid speed at which new security concerns develop can often hinder communication and cooperation among cyber security researchers. For example, in mathematics, where a few individuals may work on a particular problem, those individuals learn of each other through publication and research associations. A ten-year-old research paper on a specific mathematics problem may still be quite relevant today. In contrast, when a specific problem arises in cyber security, many researchers swarm to the problem and a research paper may be old news six months later. Academic publications do not provide the same level of communication and information access for cyber security as for traditional academia. As a result, one of the most frequent questions heard at the symposium was, "Who's doing what research where?"

Also, cyber security researchers generally work in the narrow confines of sub-topics within one specific layer of the security architecture. Although the narrow focus is necessary for researchers to become experts on particular cyber security topics, their specific expertise is only one part of the big picture. Symposium attendees were concerned that no one seems to be looking at all the layers together.

The Solutions

Cyber security researchers can find help from organizations like SURA and the CIP Project, who can maintain a large-scale view and facilitate timely communication and information access among universities, government, and industry. For example, these organizations can act as information repositories of "who's doing what research where," publish benchmarks, and can guide the establishment of standards (eg., incident definitions, minimum accepted security processes, etc.). They can also provide the structure and independent oversight for multi-university collaborative efforts (eg., anonymizing procedures, tools, and direction for a multi-university test bed that sniffs all network traffic). Further, these organizations can provide up-to-date information to both industry and university researchers.

Looking at *(Continued, Page 18)*

Higher Education's Role in Critical Infrastructure Protection

by Phil Thiel
Vice President, Dewberry and Davis

The need to protect the Nation's critical infrastructure has never been higher. Institutions of higher learning (i.e., colleges and universities) are in a unique position to contribute significantly towards this effort, particularly with regard to identifying key issues and recommending policy and unbiased technological solutions. Because these institutions likely do not have a significant stake in the technological solutions, they are a good choice to play an "honest broker" role. In addition, these institutions have a proven track record of success in providing technical expertise and research and development legwork towards the advancement of industry and government.

With the multitude of local, State, and Federal agencies now concerned with protecting critical infrastructure, a neutral third-party is an essential ingredient towards building consensus. Since these non-profit institutions are somewhat removed from the politics and daily challenges of protecting critical infrastructure, they may be an excellent choice for objectively weighing each stakeholder's need. As a trusted advisor, with their main agenda being creating solutions that meet industry's needs, colleges and universities are well positioned to create a fair and balanced end product. This approach is more likely to be embraced by stakeholders than a single entity creating a mandatory structure or standard. This approach is also more likely to strike an even balance in addressing end-users' specific needs.

Colleges and universities, being a focal point for learning and research, present an opportunity to tap intelligence motivated by more than just financial gain. These institutions also provide an army of students, led by technical experts, willing and able to do a great deal of the time consuming and necessary research and development for little cost. Upon graduation, these students would be uniquely qualified to enter the workforce and support the ongoing efforts to protect the Nation's critical infrastructure. ❖

Undergraduate Curriculum *(Cont. from Page 3)* nation-wide institutions and organizations.

Specific milestones to date include:

- Students and staff from GMU visited the US Military Academy at West Point in the summer and fall of 2003 to obtain their virtual system (lap-top version) and to inspect their new labs. Col. Daniel J. Ragsdale visited GMU on July 2, 2003 to meet with faculty and staff to discuss and advise on the curriculum and laboratory space at West Point.

- GMU faculty and graduate student Research Assistants have visited and are working with GWU by analyzing their graduate security curriculum and exercises. Two PhD candidate RAs enrolled in GWU's spring 2004 semester course to gather experience and critique their material. Discussions during the fall of 2003 with Professors Lance Hoffman and Tim Rosenberg on their Portable Educational Networks - PEN and PEN2 and curriculum material have been effective in improving GMU course development and its laboratory changes.

- A GMU graduate Denial of Service course in the fall 2003 semester used the GWU exercise set for PhD student participants to help assess the use of such exercises at GMU. Some of these students will aid in teaching the capstone course and in developing new *(Continued, Page 18)*

Information Sharing in Higher Education: Research and Education Networking ISAC

by Doug Pearson
Indiana University

Supported by Indiana University and through relationships with Internet2 and EDUCAUSE, the REN-ISAC (Research and Education Networking Information Sharing and Analysis Center) is an integral part of higher education's strategy to improve network security by providing security information collection, analysis, dissemination, early-warning, and response specifically designed to support the unique environment and needs of organizations connected to higher education and research networks.

Formalized in February 2003, the REN-ISAC supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC structure and is actively engaged in efforts such as the ISAC Council, the National Cyber Security Partnership, the EDUCAUSE and Internet2 Security Task Force, Internet2 SALSA, daily inter-ISAC and government cyber threat status meetings, and other public and private cyber security efforts.

Membership is open to all institutions of higher education. Initial funding for the REN-ISAC was provided by Indiana University (IU); with efforts underway to secure a base of funding that permits an inclusive, expense-free membership model to continue. During operational start-up, activities have focused on Internet2 members and the Abilene network. Outreach to all of US higher education will be pursued.

With various information inputs at its disposal the REN-ISAC has a unique view of the security situation in various national and international research and education networks, including the Internet2 Abilene network. The Global Network Operations Center co-located with the REN-ISAC at Indiana University monitors these networks 24x7; IU network and security engineers are among the best in the country; and the Advanced Network Management Lab at IU is involved in advanced network security research. Network instrumentation to which all of these engineers and researchers have ready access provides specific information about security events.

With the objective to codify deep and rich cyber security contact information for all US universities and colleges, the REN-ISAC is developing a cyber security registry for higher education. The primary registrant of an institution - the IT Security Officer or superior - will assign contact delegates who can act immediately, with knowledge and authority, and who are cleared to handle potentially sensitive information. Registrations will be vetted for authenticity, and currency of the information will be aggressively maintained. The REN-ISAC will use the Registry as a tool for directing potentially sensitive communications regarding early warning and active threat. The Registry will be open for use by members of the trust circle established by the Registry, and the REN-ISAC will proxy contact information to external trusted circles including other ISACs, CERTs, ISPs, law enforcement, etc.

The REN-ISAC Watch Desk, (317) 278-6630 or ren-isac@iu.edu, is staffed 24x7 to receive and disseminate timely information regarding network security vulnerability and threat in the higher education community. ❖

Building and Managing the Infrastructure Advisory Team for DHS

John C. Nemeth, Ph.D.
Vice President for Partnership Development
Oak Ridge Associated Universities

Last Autumn, Oak Ridge Associated Universities (ORAU) began a program on behalf of the Department of Homeland Security (DHS) Protective Security Division to assemble and manage a cadre of highly qualified and articulate experts from the faculties of colleges and universities with expertise in chemical, biological, and nuclear weapons of mass destruction (WMD). The experts initially appointed would come from institutions, centric to Washington, DC, nominally within four hours of direct contact with DHS.

The Infrastructure Advisory Team, as the current group of twenty-nine experts is known, will eventually have as many as 50 members. The experts would provide specifically tactical and situational advice to DHS in the event of WMD terrorist events, and would be asked to help DHS present scientifically grounded information to the public.

Therefore, this is not a "what if" exercise. Team members possess credentials as physicians, psychologists, sociologists, health professionals, Ph.D. scientists and engineers, and others. As one might imagine, the possible taxonomy of expertise quickly gets very complex when one sits back and considers all the aspects of our society that can be affected by a WMD attack. We have sought and have been signing up the very best, most experienced people we can find. I am very pleased with the outstanding quality of the folks who have chosen to become involved, and I am particularly heartened by the fact that all seem to be genuinely interested in this for our country. They are on call 24/7, so I am trying to build some redundancy into the areas of expertise to assure availability when various team members are on travel.

ORAU will continue to identify, evaluate, and contract with experts from ORAU member and other academic institutions in the Washington, DC area. I am not advertising for applicants, as those selected come highly recommended by their peers. Eventually, the team could be expanded to include academic experts from across the country, but such plans are in the future, if ever. ❖

Dr. Adebisi Oladipupo
Vice President for Research and Technology
Norfolk State University

A critical component and priority of the National Cyberspace Security Infrastructure is Awareness and Training. Quite often we focus on technical details of design and development of security infrastructure and forget the human factor necessary for a successful deployment. The criticality of education, training, and workforce development amplifies the important role higher education plays in cyberspace security. Higher education can not be content in just developing the next generation cyberspace security sensor networks but actively pursue training and policy developments that will ensure success in this lofty endeavor.

EDUCAUSE *(Cont. from Page 7)*
higher education community. Dedicated higher education professionals are kept informed through numerous EDUCAUSE publications and a comprehensive website which offers a variety of services. EDUCAUSE has worked to advance communication between institutions of higher learning and will continue to provide avenues for collaboration in the advancement of IT.

For more information: www.educause.edu ❖

Virginia Alliance for Secure Computing and Networking

The Virginia Alliance for Secure Computing And Networking (VA SCAN) is a partnership between four universities; the University of Virginia (UVA), George Mason University (GMU), James Madison University (JMU), and Virginia Polytechnic Institute (VA Tech). Joining security practitioners from these four universities are researchers and staff from the Institute for Infrastructure and Information Assurance (3IA) at JMU, the Center for Security Information Systems at GMU, and the joint GMU/ JMU Critical Infrastructure Protection Project (CIPP).

Representatives from other Virginia institutions, including Mary Washington College, Radford University, The Virginia Institute of Marine Science, The College of William and Mary, Virginia Commonwealth University, and the Virginia Military Institute advise VASCAN partners.

Some of the benefits to be gained from the Alliance are:

- Ability to leverage field-proven security tools and best practices and staff expertise
- Improvements brought about through close linkages with cyber security research, instruction, and federal and state initiatives
- Saves security program development time
- Helps avoid costs associated with security breaches
- Takes advantage of economies of scale
- Reduces security training costs

Some of VA SCAN's current product and service offerings include:

- Onsite training and security instructional materials
- Onsite consulting on a variety of security topics and an "ask the expert" email service
- Web-based toolkit of security tools and best practices
- Self-assessment checklist for Commonwealth of Virginia security standards
- A moderated mail list for general security discussions
- A VA-CIRT group for tracking security threats
- Periodic information sharing meetings and workshops (the next one is scheduled for October 11th at UVA)
- Security policy development and security awareness training

Although VA SCAN's primary mission is to help strengthen information technology security programs within the Commonwealth of Virginia's Higher Education community, we have been able to deliver some benefits to both K-12s and state government agencies and will continue to do so as our resources permit.

During its first year in existence VA SCAN has been involved in a number of information security-related activities. These included:

- Conducting consulting engagements and training sessions for a number of colleges and universities
- Partnering with the Software Engineering Institute (SEI) and ArcSight to demonstrate a more efficient and broad-based capability for the sharing of Internet security information
- Sponsoring training by SANS and SEI in the areas of incident response, computer forensics, the creation of a CSIRT, and wireless security

As recognition of VA SCAN's efforts, at the last Commonwealth of Virginia Information Technology Symposium (COVITS) the Alliance was awarded the Governor's Service Award. This award honors those public sector organizations that use technology innovatively to enhance the provision of services to its customers, realize a return on investment in terms of cost savings and cost avoidance, and improve the overall efficiency of operations.

If you would like to learn more about VA SCAN please visit its website at: http://vascan.org. Or if you have any questions or comments, please e-mail them to: vascan-services@virginia.edu. ❖

Centers of Academic Excellence in Information Assurance

The National Security Agency's (NSA) National Centers of Academic Excellence in Information Assurance Education (CAEIAE) program, established in November 1998, helps NSA partner with colleges and universities across the nation to promote higher education in information assurance (IA). Under this program, 4-year colleges and graduate-level universities apply to NSA to be designated as Centers of Academic Excellence in IA Education. Each applicant must pass a rigorous review demonstrating its commitment to academic excellence in IA education. During the application process applicants are evaluated against stringent criteria for measurement based on IA training standards set nationally by the Committee on National Security Systems. Designation as a CAEIAE is valid for three academic years, after which the school must successfully reapply in order to retain its CAEIAE designation.

The criteria are designed to measure and recognize the depth and maturity of Information Assurance (IA) academic programs, and to stimulate the development of broad-ranging IA programs to meet the varying needs of the student population, including work-force professionals, as well as the employment needs of government and industry. Institutions successfully meeting the criteria are "designated" as Centers of Academic Excellence in Information Assurance Education. The criteria are not designed to the discriminating level required of programs offering a specific "accreditation" or "certification." Accreditation and certification establish a minimum set of criteria to assure that a basic level of quality instruction is provided in a field of study. A CAEIAE goes beyond that, and serves as a model for other institutions offering IA education.

CAEIAEs receive formal recognition from the U.S. government, as well as prestige and publicity, for their role in securing our nation's information systems. Students attending CAEIAE schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program (SFS).

CAEIAE Institutions are located throughout the country-many within driving distance of major DoD installations, federal research centers, and other federal agencies. These schools serve as regional centers of IA expertise and have begun to provide more programs aimed at retooling and retaining current federal and state information

(Continued, Page 14)

1999-2002 / 2002-2005
George Mason University (VA)
Idaho State University (ID)
Iowa State University (Iowa)
James Madison University (VA)
Purdue University (IN)
University of California, Davis (CA)
University of Idaho (ID)

2000-2003 / 2003-2006
Carnegie Mellon University (PA)
Florida State University (FL)
Information Resources Management College, National Defense University (DC)
Naval Postgraduate School (CA)
Stanford University (CA)
University of Illinois, Urbana-Champaign (IL)
University of Tulsa (OK)

2001-2004
Drexel University (PA)
United States Military Academy, West Point (NY)
Georgia Institute of Technology (GA)
University of Maryland, Baltimore County (MD)
Mississippi State University (MS)
University Of North Carolina, Charlotte (NC)
Norwich University (VT)
West Virginia University (W VA)
Syracuse University (NY)

2002-2005
Air Force Institute of Technology (OH)
George Washington University (DC)
Indiana University of Pennsylvania (PA)
New Mexico Tech (NM)
North Carolina State University (NC)
Northeastern University (MA)
Polytechnic University (NY)
State University of New York, Buffalo (NY)
State University of New York, Stony Brook (NY)
Towson University (MD)
University of Maryland, University College (MD)
University of Nebraska, Omaha (NE)
University of Texas, San Antonio (TX)

2003-2006
Auburn University (AL)
Capitol College (MD)
East Stroudsburg University (PA)
Johns Hopkins University (MD)
New Jersey Institute of Technology (NJ)
Pennsylvania State University (PA)
Portland State University (OR)
Stevens Institute of Technology (NJ)
Texas A&M University (TX)
University of Dallas (TX)
University of Massachusetts, Amherst (MA)
University of Pennsylvania (PA)
University of Virginia (VA)
Walsh College (MI)

Target Washington *(Cont. from Page 4)* remain. The February 2004 ricin incident in Washington, DC, during which three Senate office buildings were closed, emerged as a case-in-point. Dr. Dan Hanfling, Director of Emergency Management and Disaster Medicine for the Inova Heath System, told the Target Washington audience that, to his chagrin, he learned of the ricin incident not through official notification but through the news media. The health system has to be in the law enforcement and intelligence loop, he argued, and viewed this as an essential part of the critical infrastructure.

Secretary Ridge said improving information sharing remains a top priority of homeland security because local governments and law enforcement represent the frontlines in efforts to deter, prevent and respond to terrorism. "The most important thing we can do at any level of government is ...preparation, preparation, preparation...share information so that people can act on it," Ridge said.

Perhaps the most remarkable aspect of our town hall meeting was the clear desire by citizens to be more involved. Several audience members asked where they could find more information to assist in homeland security efforts at both the local and national levels. Some were already volunteering and others had obtained emergency preparedness training through Computer Emergency Response Team (CERT) programs. A recent Council for Excellence in Government survey assessing citizens' attitudes toward homeland security shows that this is not a sentiment confined to the Washington region only. The poll indicates that an overwhelming majority of Americans said they were willing to volunteer. In fact, more than 20% said they would commit one to two hours every week to the task.

The challenge remains for elected and appointed officials to best keep the public's faith, energy and commitment while continuing to improve the never-ending job of homeland security both in the NCR and across the country.

Note: "Target Washington" was a joint production of George Mason University and WETA public television channel 26. Web content was provided by Washingtonpost.com, which posted a personal preparedness guide. Frank Sesno is University Professor of Public Policy and Communication and former CNN Washington Bureau Chief and anchor. GMU Faculty Research Associate Bryan Day contributed to this article. ❖

NSA Centers of Excellence *(Cont. from Page 13)* technology personnel.

In conjunction with the CAEIAE Program, the Information Assurance Directorate is a sponsor of the Colloquium for Information Systems Security Education (CISSE) and the Senior Executive Academic Liaison (SEAL). The addition of these programs helps to promote and increase the availability of information assurance education across the nation while benefiting both NSA and the partnering universities. ❖

Role of Universities *(Cont. from Page 2)* required for infrastructure planning, development, operation, and evaluation. There is a strong argument for the development of a new, dedicated infrastructure track that integrates public administration and technical disciplines to provide the balanced skill set expressly designed for infrastructure practitioners.[2]

While the first role of Universities is education, our role in infrastructure assurance does not stop there. University infrastructure assurance programs should embrace research, policy studies, public awareness, development and promulgation of best practices, and real-time/real-problem assistance to public and private infrastructure stakeholders. Universities, as trusted agents, are capable of gathering data and assisting infrastructure service providers that are often reticent to work with government organizations.

Universities can lead by example since they represent microcosms of critical infrastructure networks and system interdependencies. The campus provides an excellent location for developing and demonstrating infrastructure assurance practices and tools. And universities are one of the most challenging venues vis-a-vis infrastructure assurance given the openness needed for academic pursuits. Thus the university example advances state-of-the-art approaches to achieving security while at the same time protecting the freedom of the individual. If we can effectively protect university infrastructure, we can apply the lessons learned to secure many other types of open institutions.

As an example, James Madison University is developing a broad program that combines infrastructure and cyber assurance activities, leveraging our established information security program. We seek to cultivate a balanced ensemble of cyber and physical pursuits contributing to infrastructure assurance. To coordinate many diverse, interdisciplinary contributing activities within the University, we have established a new Institute for Infrastructure and Information Assurance (IIIA). The institute administers activities of two major grants, the Critical Infrastructure Protection (CIP) federal grant in partnership with George Mason University, and the (Virginia) Commonwealth Information Security Center (CISC) grant. We have begun developing new curricula in the infrastructure assurance discipline beginning with an infrastructure survey course and moving toward an information analyst track. Under the CIP project, we are developing new infrastructure network risk assessment tools at the same time engaging in actual system risk assessments to ensure the usefulness of the tools. Our risk assessment clients presently include university network IT operations and a local municipal electric power system, both efforts tightly coupled with the risk tool development. We are providing public awareness through visiting scholar forums and awareness presentations to local public service organizations. Our research program includes projects that span the prevention, protection and response infrastructure and information assurance strategies. Research is geared to foster the participation of both graduate and undergraduate students.

Addressing infrastructure issues as an explicit university program including instruction and research opportunities provides a major force for real advances in the improvement and protection of our critical infrastructures. The enormous, multifaceted nature of infrastructure systems, services, policy, and economics demands university programs that emphasize interdisciplinary thinking, communication, team building, and problem solving. We must break down the barriers separating the hard sciences, law, public policy, business and economics to develop non-traditional degree paths and collaborative research venues to successfully prepare the next generation of infrastructure professionals. ❖

[1]National Security Agency; List of Centers of Academic Excellence in Information Security
[2]R.G. Little, Educating the Infrastructure Professional: A New Curriculum for a New Discipline, National Research Council

The Office of Science and Technology of the Embassy of Switzerland, the Swiss International Relations and Security Network (ISN) at the Swiss Federal Institute of Technology (ETHZ), and the Critical Infrastructure Protection Project (CIPP) at the National Center for Technology and Law at the George Mason University School of Law hosted an event on March 11th to celebrate the publication of the Critical Information Infrastructure Protection (CIIP): Issues and Prospects, the 2004 International CIIP Handbook. First released in 2002, the Handbook was substantially expanded for its 2004 debut focusing on CIIP in fourteen countries. For this 2004 edition, members of the CIP Project Staff, John McCarthy, Emily Frye, Anne Mitchell, and Jordana Siegel, provided editorial support and updated the U.S. Country Survey.

The dependence of modern industrialized societies on a wide variety of national and international information infrastructures was the impetus for creating the Handbook in an effort to inform security policy analysts, researchers, and practitioners about the international CIIP landscape. The Handbook brings together information on national policy approaches to CIIP and methods/models used to assess various aspects of critical information infrastructure (CII).

The occasion, held at the Swiss Embassy, featured presentations by U.S. and international CIIP experts, including: Myriam Dunn and Isabelle Wigert, authors of the publication and researchers at the Center for Security Studies at the ETHZ; Michel Maechler of the Global Information and Communication Technologies Policy Division at the World Bank; and, Paul Kurtz, former Special Assistant to the President for Critical Infrastructure Protection and Executive Director, Cyber Security Industry Alliance.

Legal Insights *(Cont. from Page 6)*

Infrastructure Protection Challenges in Securing Control Systems. GAO-04-140T (Washington, D.C. October 2003).

[4]United States Department of Justice Press Release. 28 October 2003.

[5]Prosser, William L., and Page W. Keeton. Prosser and Keeton on The Law of Torts. St. Paul: West Group, 1984. 170.

[6]Nevada Revised Statutes §463.790.

[7]Chemical Facilities Security Act of 2003, S. 994, 108th Cong. (2003).

[8]Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996).

[9]Gramm-Leach-Bliley Act, Pub. L. No. 106-102 (1999). ❖

Innovative Research in Security: Wireless P2P Settings

ABSTRACT

Markus Jakobsson
Principal Research Scientist, RSA Laboratories

With an increasing sophistication of attacks on the infrastructure, whether for monetary, political or other reasons, the awareness of the need for appropriate security design is growing. Wireless peer-to-peer systems pose particularly difficult problems, as attackers can easily disappear and reappear; nodes are not in constant connection with trusted authorities; and have limited resources.

We will describe three aspects of wireless peer-to-peer routing for which attacks need to be averted. Our first example is when one-hop communication links (such as standard cellular telephony, where devices communicate directly with base stations) are replaced by multi-hop wireless routing. Mobile nodes then send data to a cell tower via peers located between the node and the tower. Communication in small hops has the potential of reducing the total power consumption, since the power needed to transmit a message depends on the distance it needs to be transmitted as a power of two or more. This, in turn, allows for smaller and cheaper batteries, and thereby smaller and cheaper mobile devices. In order to avoid that selfish nodes ask others to route for them, but refuse to help others, one can use an incentive scheme in which intermediary nodes get paid each time they help routing a message [1,2], causing selfish nodes to run a deficit. An issue orthogonal to that of providing incentives for collaboration in routing schemes is that of protecting the privacy of the nodes and their users, studied in [3]. The lack of such protection would allow an attacker to determine where victim nodes are located relative to other nodes, and to known fix-points. This may be used to spy on people and organizations, where the spy may be any peer node in the network. To address this problem, one can use periodically changing pseudonyms for each node, making it difficult to trace their movements. However, this complicates the maintenance of routing tables, making the balancing act between the robustness of the system and the privacy of its users delicate.

A third security issue of wireless routing is that of protecting against attackers who wish to partition the network, i.e., isolate victim nodes from the rest of the network. In [4], it was described how an attacker can manipulate the routing tables of peer nodes, and thereby cause them to route data incorrectly. This may be used both to isolate victim nodes and to re-route traffic for the purpose of traffic analysis. While the effects of such attacks can be limited using authentication mechanisms, it is shown in [4] that the reliance on any technique involving computation at victim nodes will allow an attacker to partition the network by instead performing a denial of service attack on the power supplies of victim nodes. Light-weight cryptography may be helpful in avoiding attacks, but is not a panacea.

We have briefly described three new security problems, all relating to wireless routing between peer nodes, some of which may misbehave. In order to make the nodes collaborate with each other, protect them against intrusions of their privacy, and maintain network connectivity, we look beyond traditional cryptography for answers. The techniques used to address these problems may be useful in a much wider range of settings than wireless peer-to-peer systems, and the research promises the potential to address security problems in situations where traditional techniques fail.

BIBLIOGRAPHY

1. M. Jakobsson, J.-P.Hubaux and L. Buttyan, "A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks", Financial Cryptography '03.
2. N. Ben Salem, L. Buttyan, J.-P. Hubaux, M. Jakobsson, "A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks", ACM MobiHoc '03
3. S. Capkun, J. P. Hubaux and M. Jakobsson, "Secure and Privacy-Preserving Communication in Hybrid Ad Hoc Networks", EPFL-IC Technical report no. IC/2004/10, January '04.
4. M. Jakobsson, S. Wetzel, B. Yener, "Stealth Attacks on Ad-Hoc Wireless Networks", IEEE VTC '03. ❖

SURA *(Cont. from Page 8)* cyber security from all aspects, it is immediately noticeable that cyber security issues mirror those in physical security: how to balance security and privacy fears; how to secure not only the facility, but also everything going in or out; how to best detect intruders; how to manage sharing and handover of information among organizations without compromising security; and the list goes on. (In fact, some researchers have seen these similarities and have begun to study the idea of a Cyber Security First Responders unit.)

This all-encompassing view of cyber security may allow it to mimic concepts from other critical infrastructures; and with access each other's research, physical security can learn from cyber security. For example, researchers at James Madison University have created a very simple electronic grid model, including a bucket truck and two repairmen, to model critical infrastructure damage and repair. This seemingly simple research model has the potential to provide guidance to numerous critical infrastructures. With the support of wide-reaching organizations, industries could have timely access to such research.

The ever-evolving and broad nature of the cyber security discipline hinders individual researchers from finding solutions to the overarching problems of security architecture. Traditional academic methods of communication and cooperation, like conventional academic journals, do not provide cyber security researchers with timely access to information. It is necessary to adopt a more holistic view, bringing together many security elements to facilitate access to information and promote communication. ❖

Undergraduate Curriculum *(Cont. from Page 9)* bridging courses, act as mentors, and help develop any required additional software.

- JMU has developed a new undergraduate course, "Information Security," that debuted in the 2004 spring semester. This course is one pre-requisite to the capstone course.

- A considerable amount of energy has gone into the design of a new security lab to support the capstone exercises.

We therefore intend to graduate students capable of excelling in careers as *information security engineers* or as *computer science graduates* with a specialization in *computer and network security* and, by collaborating and integrating work from other institutions, reduce costs in duplication of curricula. ❖

Homeland Security Centers of Excellence

The Department of Homeland Security (DHS) expects the United States academic community to play an integral role in securing the Nation. To facilitate this involvement, the Office of University Programs, within the Science and Technology division of the Department, will establish university-based Homeland Security Centers of Excellence (HS-Centers). The purpose of these Centers is to provide a locus to attract and retain the nation's best and brightest academic scholars in pursuit of homeland security related disciplines. Through this program, the Department of Homeland Security and partner universities will bring together the nation's best experts and focus its most talented researchers on a variety of threats that include chemical, biological, nuclear and radiological, explosive and cyber terrorism.

The HS-Centers will complement other programs within the Department (including the Homeland Security Advanced Research Projects Agency) and in other federal agencies that fund projects-focused research aimed at the development and deployment of specific homeland security technologies and capabilities. The selection of the HS-Centers will be coordinated with other federal agencies to minimize duplication of effort and maximize coordination of expertise and resources.

In November 2003 DHS announced that the University of Southern California (USC) was chosen as the first HS-Center. The Department anticipates providing the University with $12 million over the course of the next three years for the study of risk analysis related to the economic consequences of terrorist threats and events.

Welcome and Introductions - Staff:

We are extremely happy to introduce new members of our staff.

Felecia Hairston joined our staff as the Director's Executive Assistant.

Amy Cobb is the new Senior Project Associate and the project's Events Coordinator.

Private Sector Coordination:

Jen Marthia joined the team as a Senior Project Associate, working on private sector coordination and strategic planning.

National Capitol Region (NCR):

Christine Pommerening, PhD, joined the staff as a CIP fellow and post doctorate.

Jordana Siegel has taken over the Senior Project Associate position for the NCR project.

Andrew Rail joined the team as the NCR's Research Associate.

Celebrations and Milestones:

Anne Kilburn Dailey (Mitchell) was promoted to Senior Legal Research Associate in March of 2004.

Anne Mitchell, now Anne Kilburn Daily, was married on Saturday, April 3, 2004 to Joseph Daily. Best wishes to them on this wonderful event and their new life together!

Congratulations to **Emily Frye**, Associate Director for Law and Economics on the birth of her new son Richard Alton! Richard was born Monday, March 29, 2004 to two proud and very tired parents.

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.