The Critical Infrastructure Protection Program October 2005 / Volume 4, No. 4

THE CIP REPORT

CIP Practitioner Training and Education

Newsletter Editorial Staff

Editors

Jessica Milloy

Jeanne Geers

Staff Writers

Amy Cobb

Randy Jackson

Colleen Hardy

Maeve Dion

JMU Coordinators

John Noftsinger

Ken Newbold

Publishing

Zeichner Risk Analytics

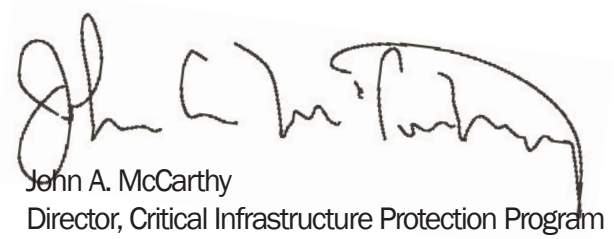
Contact: cipp01@gmu.edu
703.993.4840
If you would like to subscribe to *The CIP Report* please click here.
Visit us online for this and other issues at http://cipp.gmu.edu

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

During the past three years *The CIP Report* has been in distribution, we have received numerous inquiries from readers around the country, requesting referrals to programs similar to our program here at George Mason University. Additionally, a large number of our readers have requested information on education opportunities for practitioners in the field of Critical Infrastructure Protection (CIP). In the years since the CIP Program was founded, we have seen dramatic growth in the number and types of opportunities for both current and future practitioners, and in this issue, we highlight many of the different programs available from government bodies, private for-profit groups, and educational institutions. As the founding Director of the CIP Program, I take great pride in the interdisciplinary and multi-institutional model that we have grown and matured over the past few years, and the number of informal calls I have received from other groups wishing to establish programs similar to our own.

While many of us entrenched in this field arrived via circuitous routes, drawing on diverse backgrounds and experiences, new curriculums, degrees and professional associations are changing the field by enabling practitioners to grow and refine their resumes and creating new generations of professionals, straight out of higher education institutions. As the aftermath of Hurricane Katrina unfolds, more CIP issues are exposed, continuing to draw greater awareness to the complexity of the challenges practitioners and educators in this field face. While no amount of education or training can prevent incidents of national significance, programs such as those we feature in this issue will use these lessons to better prepare the practitioners of the future. The interdependency issues so clearly on display in this disaster will turn into case studies and topics of class discussion in the coming months and years, better informing and preparing future CIP leaders.

In an effort to provide insight into the diverse array of training and education opportunities within the CIP field, we are pleased to highlight the Center for Homeland Defense and Security at the Naval Postgraduate School, CERT Training and Education efforts, and FEMA's Emergency Management Institute. In addition, we have a listing of degrees and certificates available around the nation from a variety of institutions. As an example of the many courses taught at institutions around the country, I have included course and syllabus information from a class I am currently teaching for Syracuse University's School of Information Studies. We also include information on a K-12 education initiative, the unique world of hacker conferences, and a recap of the National Policy Forum, in which the CIP Program participated. We hope you enjoy this issue and, as always, we welcome your questions and suggestions as we continue into our fourth volume of *The CIP Report*.



John A. McCarthy
Director, Critical Infrastructure Protection Program
George Mason University, School of Law

The Center for Homeland Defense and Security

Ted G. Lewis, Ph.D.
Rudy P. Darken, D.Sc.
Naval Postgraduate School

The Center for Homeland Defense and Security (CHDS), created in 2003, provides a range of educational services for the US Department of Homeland Security (DHS). These include Mobile Education Teams for Governors and their executive staffs, creation of a unique digital library with emphasis on homeland security, research and development of distance learning content and technologies including modeling and simulation for use in educational games, the first Master's Degree program in homeland security and defense, and the first hybrid network-based/in-resident educational program for next generation state and local homeland security leaders. CHDS is described at www.CHDS.us, and includes an application process for candidates interested in applying for a limited number of all-expense paid positions in the graduate degree program.

CHDS initiated the Master of Arts (MA) degree program in January 2003 and has graduated over 50 students as of July 2005. The 18-month program is unique in its structure and delivery mechanism. The purpose of this article is to describe the MA degree program and discuss what has worked and what has not worked so that others may benefit from our experience.

Curriculum

From the beginning, the 18-month hybrid in-resident/distance learning degree program was designed for working professionals - state and local leaders destined to be the next-generation executives in emergency management, law enforcement, public safety, public health, and public administration. The curriculum focuses on prevention of terrorism and acts of terror, rather than how to improve response or readiness of first-responders. The curriculum focuses on strategies and policies that lead to prevention of attacks rather than the clean up afterwards.

A second major departure from most other programs in homeland defense and security derives from the students themselves. Students are fully employed and put in 10-12 hours per day while on the job, and therefore have time for approximately 10-12 hours per week to participate in their studies. Although tuition, books, travel, computer equipment, and lodging are paid by DHS, students must commit their valuable off-the-job time to this program. Consequently, delivery is by a combination of in-residence and non-resident learning. Students enroll in two or three courses per quarter, and spend 2 weeks of each quarter in Monterey attending class 8 hours per day. The first 3 days are devoted to completing the previous quarter's courses, and then the next 8 days are devoted to beginning the next quarter's courses. Students typically devote their two-day weekend to study.

Upon admission to the program, students are engaged in a rigorous orientation process leading up to the graduate credit courses, shown in Table 1 *(see page 3)*. The premise of the curriculum architecture is that "threat" subjects should be presented first, followed by specialization courses, and finally, synthesis courses and the thesis. Therefore, Introduction and Asymmetric Conflict precedes courses on information technology, comparative governments, critical infrastructure protection, intelligence, and legal issues. Then the emphasis shifts toward synthesis - the final phase where students are encouraged to synthesize their own solutions to the problems posed by the foregoing courses. *(Continued, Page 3)*

CHDS *(Cont. from Page 2)*

Delivery

Students attend classes 8 hours per day while in residence at the Naval Postgraduate School during each 2-week period. The remaining 8-10 weeks of the quarter are spent online. Every student receives a laptop computer, iPOD player, login and password for access to the learning modules at www.CHDS.us and instruction on how to use the technology. Student and instructor performance is carefully monitored and measured by an independent curriculum evaluator. This rigorous feedback is used to determine the effectiveness of both machines and people in the acquisition of knowledge and skills - before and after each course. As a consequence of this rigorous process the curriculum and delivery in hybrid format has rapidly evolved to where it is today, and will continue to improve over time.

Initially, we thought that the best way to deliver complicated policy and strategy education to busy executives was to pre-load the courses with fully packed lectures during the face-to-face in-residence portion and use the Web for collaboration and testing. The more ambitious instructors even proposed using "scenarios" online to engage students in experiential learning. The first generation delivery strategy quickly failed for a number of reasons: scenario development is difficult and expensive, instructors viewed the online collaboration as an extension of classroom discussions, or instructors were uncomfortable with the technology. The first generation "teach face-to-face, and discuss online" gradually evolved into the reverse mode: "teach online and discuss face-to-face." This transition continues today.

In general, technology is no substitute for face-to-face in-resident learning, but appropriate technologies can be used to enhance or magnify face-to-face learning. In a sense, technology can be used to extend face-to-face learning so that learning can continue in a virtual sense.

Our evaluation process has uncovered some unexpected results. For example, audio recordings delivered by iPOD players is ranked the most effective for delivery of readings and lectures. Streaming media is second, while in-class lectures and the traditional textbook rank third. Students prefer the time and space shifting made possible by mobile devices such as the iPOD. They also prefer timesaving techniques provided by streaming media, because they can fast-forward, reverse, and replay online lectures provided by this format. Finally, textbooks appear to be most valuable as a reference rather than a learning tool!

(Continued, Page 17)

TABLE 1. MA Degree Curriculum: Course Numbers and Credit Hours

FALL	SO 3210 (4) Asymmetric Conflict and Homeland Security	NS 3180 (4) Introduction to Homeland Security	NS 2013 (2) Policy Analysis & Research Methods
WINTER	IS 4010 (4) Information Technology Management for Homeland Security	NS 3028 (4) Comparative Government for Homeland Security	NS 4081 (2) Research Colloquium
SPRING	CS 3660 (4) Critical Infrastructure: Vulnerability Analysis & Protection	NS 3027 (4) Special Topics in Homeland Security	NS 0810 (0) Thesis Research
SUMMER	NS 4156 (4) Intelligence for Homeland Security: Organizational and Policy Challenges	NS 4881 (4) Law Enforcement & Judicial System Issues in Homeland Security	NS 0810 (0) Thesis Research
FALL	NS 4755 (4) Strategic Planning and Budgeting for Homeland Security	NS 4133 (4) Psychology of Terrorism and Fear Management	NS 0810 (0) Thesis Research
WINTER	NS 4233 (4) Capstone in American Government for Homeland Security		NS 0810 (0) Thesis Research

Building a Cadre of Skilled Practitioners for Critical Infrastructure Protection

Barbara Laswell, PhD
CERT® Training and Education Manager
Software Engineering Institute, Carnegie Mellon University

Knowledge in Depth for CIP Defense in Depth


Barbara Laswell

Creating knowledge in depth for defense in depth to protect critical infrastructures is a key goal of CERT® Training and Education. To fulfill its vision of an Internet community of practitioners that is aware, knowledgeable, trained and educated in information assurance and network defense, the group has established initiatives targeted at current and future workforce development. Current initiatives include equipping those responsible for protecting networks with skills in computer forensics and incident response that are based on best practices and processes, which CERT has developed in its work since 1988 with government, industry, and academia, both in the U.S. and internationally.

The Need for Qualified Practitioners in CIP

Incident analysis and management has increasingly included a strong forensics component. Although forensics practices, methodologies, tools, and analysis techniques are well established for host-based systems, the state of the practice of forensics is immature for networked systems, complex distributed systems, and the Internet. Recent changes in U.S. law have resulted in an increase in prosecution of cyber-related crime accompanied by a closer scrutiny of methodologies for cyber forensics. CERT's contributions to the forensics field are to:

- create a knowledge base of network forensics practices, methodologies, tools for use by law enforcement, incident response teams, first responder IT staff, and system and network operators;
- provide cyber forensics technical assistance to federal civilian agencies and state and local government;
- build a cyber forensics training and certification program;
- perform research and development to examine emerging technologies and associated cyber forensics techniques; and,
- establish a cyber forensics lab for research and training and a cyber forensics resource center for law enforcement and forensics analysts.

Building Practitioner Skills

To help practitioners gain the skills they need, CERT provides training in incident management and forensics, network security, and enterprise risk management. Practitioners can earn certification in incident handling and become a CERT®-Certified Computer Security Incident Handler. *(See sidebar CERT® Courses).*

(Continued, Page 5)

CERT® Courses

First Responders Guide to Computer Forensics
Creating a Computer Security Incident Response Team
Managing Computer Security Incident Response Teams
Fundamentals of Incident Handling
Advanced Incident Handling for Technical Staff
Information Security for Network Managers
Information Security for Technical Staff
Advanced Information Security for Technical Staff
OCTAVE Training Workshop

CERT *(Cont. from Page 4)*

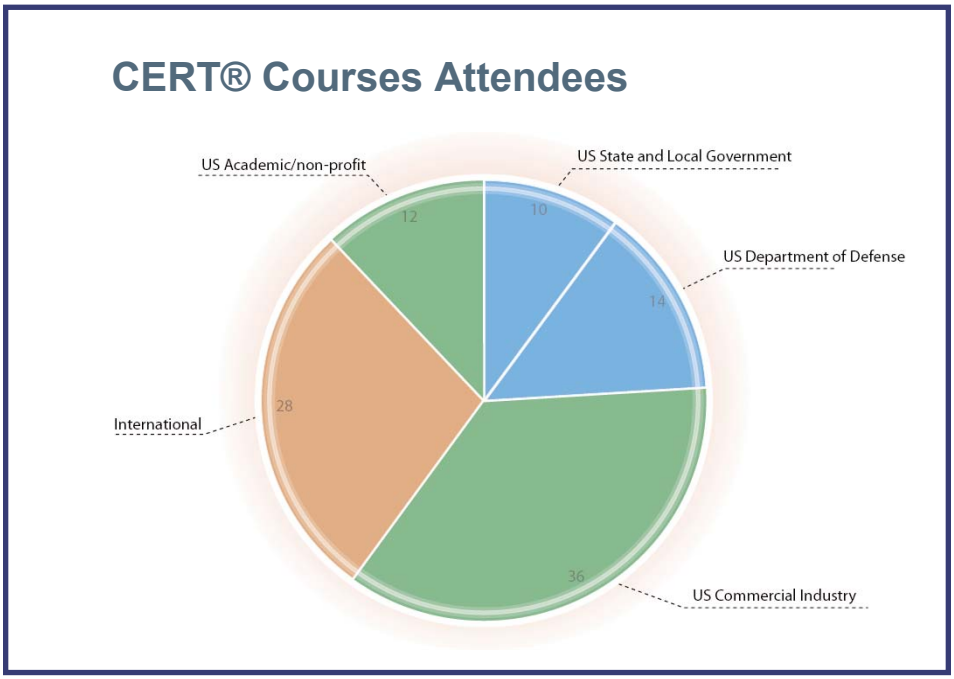
Anytime, Anywhere Learning: CERT® Virtual Training Environment

Maintaining an information assurance and computer forensics skill set across a distributed organization is financially and logistically challenging. The CERT® Virtual Training Environment allows technical staff to practice - and master - information assurance, cyber forensics, and other information security-related tasks anywhere at any time. Organized in a web-based knowledge library format, VTE includes documents, captured demonstrations of subject matter experts interacting with systems and software, recorded course lectures featuring instructors interacting with students, and hands-on labs for skills application and problem solving in a "safe haven" virtual sandbox.

Train as Individuals, Practice as Teams

Critical infrastructure protection requires individuals who have mastered the necessary cyber security and incident skills but who also have trained as members of a team. CERT has worked with U.S. government organizations to provide realistic scenarios running on virtual networks that simulate functioning enterprise networks:

- *Virtual Network Assessment* - a scenario-based testbed for practicing information assurance skills and required competencies in security improvement teams;
- *Information Assurance Exercise* - operational survivability practice with teams remotely distributed. Teams must respond to a rapidly changing environment, real-world threats, and network attacks that simulate actual conditions.



Evaluating and Improving CIP Capabilities

So how can the capabilities of cyber response teams be evaluated and improved? CERT has helped to develop certification and accreditation metrics and processes for U.S. DoD Computer Network Defense Service Providers and is currently working with the National Cyber Security Division in the Department of Homeland Security to develop a set of metrics for use by computer security incident response teams (CSIRTs) in U.S. federal civilian agencies and state and local government. Free resources to help response teams and practitioners responsible for CIP can be found at http://www.cert.org/csirts/.

CERT's reach is global, and course attendees represent a wide variety of organizations. *[See sidebar CERT® Courses Attendees.]*

(Continued, Page 15)

CIP: An International Issue

Did you know that CERT has provided

- Support to the Olympic Games and National Special Security Events
- Support to U.S. Bilateral and Multilateral Delegations on Critical
- Infrastructure Protection and Cyber Terrorism
- Training to the Army Reserve Information Operation Command
- Training to state agencies: Florida, South Carolina, California
- Training internationally: Japan, India, Algeria, Morocco, Qatar

FEMA's Emergency Management Institute

Through its courses and programs, FEMA's Emergency Management Institute (EMI) serves as the national focal point for the development and delivery of emergency management training to enhance the capabilities of federal, state, local, and tribal government officials, volunteer organizations, and the public and private sectors to minimize the impact of disasters on the American public. EMI curricula are structured to meet the needs of this diverse audience with an emphasis on how the various elements work together in emergencies to save lives and protect property.

Instruction focuses on the four phases of emergency management: mitigation, preparedness, response, and recovery. EMI develops courses and administers resident and non-resident training programs in areas such as natural hazards (earthquakes, hurricanes, floods, dam safety), technological hazards (hazardous materials, terrorism, radiological incidents, chemical stockpile emergency preparedness), professional development, leadership, instructional methodology, exercise design and evaluation, information technology, public information, integrated emergency management, and train-the-trainers.

Approximately 5,500 participants attend resident courses each year while 100,000 individuals participate in non-resident programs sponsored by EMI and conducted by state emergency management agencies under cooperative agreements with FEMA. Another 150,000 individuals participate in EMI-supported exercises, and approximately 1,000 individuals participate in the Chemical Stockpile Emergency Preparedness Program (CSEPP). Additionally, hundreds of thousands of individuals use EMI distance learning programs such as the Independent Study Program.

To take a course at EMI, applicants must meet the selection criteria and prerequisites specified for each course. Participants may not take the same course more than once. Enrollment in EMI courses is generally limited to U.S. residents; however, each year a limited number of international participants are accommodated in EMI courses.

EMI is located at the National Emergency *(Continued, Page 15)*

Steve Sharro, Emergency Management Institute Superintendent

When disasters and emergencies strike, many different organizations must work together to protect property and save lives. Ensuring and enhancing this interoperability is the goal for FEMA's Emergency Management Institute (EMI). A component of the United States Fire Administration, EMI is located on the National Emergency Training Center (NETC) campus in Emmitsburg, Maryland, 75 miles north of Washington, D.C.

EMI staff provide training to enhance U.S. emergency management performance through a nationwide program of resident, field, and distance learning activities. Over 5,000 students attend resident courses at EMI each year while thousands participate in field training sponsored by EMI and conducted by State emergency management agencies. Hundreds of thousands more use EMI web-satellite television, and text-based distance learning programs.

Being ready to deal with all types disasters and emergencies is more critical now than ever before. The staff and faculty of EMI are proud to be part of this effort and committed to the FEMA goal of "A Nation Prepared."

Legal Insights

K-12 Education and Critical Infrastructure

Randy Jackson
CIP Program

***"All who have meditated on the art of governing mankind have been convinced that the fate of empires depends on the education of youth."* Aristotle**


Randy Jackson

Is Aristotle suggesting that education is part of a nation's critical infrastructure? Certainly we could look at school buildings as critical infrastructure in the sense of any large public facility. But what about the education system - the techniques, policies and pedagogical structure? Can something that is not "infrastructure" in a literal sense be, nonetheless, a "critical infrastructure"? It is an issue that appears from time to time as policymakers try to take inventory as to what constitutes the entirety of a nation's critical infrastructure. One can easily point to such things as nuclear power plants, bridges, ports and energy plants on the physical side; and crucial IT systems such as SCADA on the cyber side. But if the inventory is to include all "things" that are crucial to the continued functioning and prosperity of a nation, the list could expand - for example international commercial trade regimes, environmental quality and a vibrant education system. This is an issue that is difficult and perhaps evolving, but one important to a nation trying to protect all of its critical infrastructure with limited resources; and more broadly a nation trying to understand itself in terms of what vitally matters. Perhaps it is not the "critical" part that is debatable, only the "infrastructure" part.

There is also a temporal aspect to this issue. If a nuclear power plant explodes, there are instantaneous, real consequences. Such consequences include the immediate deaths, injuries and destruction caused, as well as the disruption created by the loss of power. There is also the opportunity cost of having to expend resources to control the damage and recover. If the education system were eliminated today, not through an attack on a school or some such event, but rather was simply cancelled, the result would be different. Unlike the nuclear power plant scenario, no one is hurt or killed; no disruption occurs to the functioning of the society at that moment. But what happens when those who now are not educated come of age? The threat manifests itself later, more subtly, as the society collapses under its own ignorance. Again, this is no insight - societies that fail to educate the next generation fall. It is critical that a functioning society maintain a vibrant education system capable of preparing the next generations to become contributing members of the social fabric. But perhaps it is partially this temporal quirk that distinguishes education as "critical" without becoming "critical infrastructure."

However, perhaps subsections of a national education system can be seen as critical infrastructure. Education is a giant topic; to discuss it is to make reference to a myriad of systems and relationships. Even if we limit ourselves to the public K-12 education system (to reflect the nation's public role), we are addressing an extremely disparate and diverse entity. But although funding and curricula reflect the realities of local communities, there are certain skills that all school systems recognize as necessary for an individual to actively take part in the economic and political systems of the country. For example, he or she must be able to read. Therefore, without exception, American public schools throughout the *(Continued, Page 8)*

Legal Insights *(Cont. from Page 7)* country teach students to read. Perhaps herein could lie a glimpse into what part of the overall education system might be "critical infrastructure" - those aspects deemed crucial to an individual's participation in the larger nation's economic and political systems. Certainly a failure to be so trained will ultimately cause severe damage to the nation as a whole. However, how do we measure the threat to the nation in terms of numbers? That is to say, how many bad school systems does it take to truly impact the nation? Finally, how far should this go - should agencies responsible for homeland security such as DHS play an active role in curriculum development?

Perhaps a better way to look at the potential role of education as "critical infrastructure" is to ask what direct role it can play in an area already so designated, i.e., cyber security. We can ask what role the education system plays in the furthering of cyber security today. In this light, we can hone in on two very specific aspects of the current efforts to "harden" the US against cyber threats: creating more sophisticated computer users and producing more technology experts.

The cost to the US economy of successful phishing attacks has been estimated at various levels from $150 million[1] to $1.2 billion.[2] Technical strategies have been proposed, studied and in some cases implemented[3] in an attempt to stop such activity. However, phishing can also be stopped by sophisticated consumers avoiding the invitations that phishing thieves send out. Here is a role for the public education system that is applicable across the myriad of school districts: hardening the cyber network by eliminating the key weapon of phishing perpetrators, i.e. unsophisticated computer users. In this way, education (or at least a specific subsection of it) is transformed into a part of the overall toolbox needed to harden the nation's cyber network. This particular aspect of the education system becomes not only "critical," but in its attachment to the protection of the cyber network system, it becomes "critical infrastructure protection."

Another critical role education plays in the protection of critical infrastructure (in this case both the physical and cyber versions) is the training and development of new experts in engineering, computer science, mathematics and related fields. Without the on-going development of cutting-edge technology experts, the US risks falling behind not only her competitors abroad, but also her enemies at home (or abroad). The personnel portion of critical infrastructure protection is the glue that holds the whole structure together. Without well-trained individuals ready to think about and implement technical, as well as policy, remedies to the threats the nation faces, any attempt to build real critical infrastructure protection regimes and/or technologies will be a non-starter. It is in the creation of a continuous stream of professionals that education's "critical" nature also stretches into "critical infrastructure protection."

But there is more to this equation.

"The aim of education is the knowledge not of fact, but of values."

Dean William R. Inge
Professor of Divinity
Oxford University, 1907 - 1911

Creating more computer-savvy consumers and more experts in various areas of technology will only contribute to the advancement of critical infrastructure protection if such individuals use such skills and knowledge in a positive way. Training more hackers and teaching people how to better dupe the public through phishing scams certainly will not increase the nation's cyber security. The question emerges as to whether teaching students how to more sophisticatedly use a computer should be undertaken without also introducing some sort of "ethics" training as well.

Perhaps the issue has come full circle. We began by looking at the education system as a whole as critical to a nation, but not, as a whole, a critical infrastructure. However, looking more closely at some specific examples of education it can be argued that a part of education is, in fact, critical infrastructure: e.g., cyber security through better "computer hygiene" and the *(Continued, Page 16)*

Institution	Program
American Public University System	Master of Arts / Bachelor of Arts in Homeland Security
Community College of Denver	Public Safety Management Associate in Applied Science Degree
Corinthian Colleges, Inc.	Homeland Security Specialist Diploma
Curry College	Certificate in Homeland Defense
Cyber Defense Training Center	Center for Systems Security and Information Assurance
Fairleigh Dickinson	Global Security and Terrorism Certificate
Fairmont State Community and Technical College	Associate in Applied Science Degree in Homeland Security
George Mason University National Center for Biodefense	Graduate Biodefense Degrees and Graduate Certificates
George Washington University Center for Excellence in Municipal Management	Homeland Security Certificate For Municipal Managers
Idaho State University	National Information Assurance Training and Education Center
Iowa Central Community College Homeland Security Training Center	Basic Homeland Security Training
James Madison University	Institute for Infrastructure and Information Assurance
John Jay College of Criminal Justice	Interdisciplinary M.A. Terrorism Certificate Program
Kaplan College	Terrorism and National Security Management Certificate
Lamar Institute of Technology	Associate of Applied Science in Homeland Security
Myers University	Certificate in Homeland Security
National Graduate School	Homeland Security Concentration offered within Master of Science, Quality Systems Management
Naval Postgraduate School	Homeland Security Master of Arts Program
Northern Virginia Community College	Homeland Security Operations Specialist
Purdue University, Homeland Security Institute	Area of Specialization in Homeland Security
Sonoma College	Certificate in Homeland Security and Associate of Applied Science in Administration of Justice and Homeland Security Programs
Southwestern College	Bachelor of Science Degree in Security Management
University of Missouri-Rolla	Critical Infrastructure Protection / Area of Excellence
University of New Haven	Master of Science in National Security and Graduate Certificate in National Security
University of Tennessee	Center for Homeland Security and Counter-proliferation Program
University of Washington	Masters in Strategic Planning for Critical Infrastructures - Leadership Program for Homeland Security

The School of Information Studies at Syracuse University is recognized as an international leader in the information field. The school was the first of its kind in the nation, and maintains an established national ranking for its academic programs, as well as considerable demand for its education, its research, and the skills of its graduates. The school offers four different undergraduate degrees, two of which are in conjunction with related programs. There are ten separate graduate options, from a Certificate of Advanced Studies in School Media to a PhD in Information Science. Additionally, the faculty of the school crosses disciplinary boundaries to integrate the common elements of information management in business, government, education, and nonprofit settings, including the relationship of information and knowledge, electronic and traditional libraries, information systems and technology, information resources management, information policy and services, and the study of information users. Following is a syllabus for a course being offered by the school this semester.

Information Security Policy: Implications for Critical Infrastructure Protection
IST 728, Fall 2005
Syracuse University, Greenberg House, Washington, DC

Instructor: John A. McCarthy

Course Description: The course provides an in-depth examination of critical infrastructure and information security policy as they have evolved within the Federal government and private sector. The extensive interplay between these two disciplines will be explored in depth. Various security program "perspectives" such as information sharing, information assurance, law enforcement, critical infrastructure protection, public/private partnership, vulnerability and risk assessment, intelligence and homeland security/homeland defense will be explored and contrasted. Using source material and contemporary thought pieces, key legislative and policy documents will be discussed in the context of current policy-making structures and the effect of policy and business governance-making processes on managerial and technical outcomes.

Among the topics covered are: the etiology of CIP/IS policy, CIP/IS policy-making frameworks, current status and trends in security oversight, emerging issues in the management of information security processes, organizational responsibility for security management, national organizational frameworks for homeland security (CIP/IS constructs), sources of data about federal/private sector CIP/IS resources, concepts of strategic infrastructure policy planning, legal implications for federal and private sector managers, employee and citizen privacy, and trusted services.

Course Learning Objective: To provide the student with an analytical framework (historical, legal, economic, and technical) from which existing and future critical infrastructure protection and information security (CIP/IS) policy requirements can be accessed. This framework also will aid in evaluating the myriad technical security solutions being offered to both public and private sector IT/IS, CI practitioners today.

INFORMATION SECURITY SPECIALIZATION OF STUDY

The specialization in Information Security (InfoSec) provides students with a greater level of understanding and competence in public and private sector best practices of providing information security in the following dimensions: physical, operational, data, and personnel.

The School of Information Studies is committed to preparing technically sophisticated information managers who understand that information is an essential resource for people and organizations that must be used and managed effectively. As the first school in the country to offer a master's degree in information management, Syracuse University is a leading center defining both the theory and practice of information management.

Reprinted from the ***Richmond Times-Dispatch***

Securing Infrastructure: Telecoms Must Take Steps To Ensure Communications

JOHN MCCARTHY
GUEST COLUMNIST Sep 11, 2005

Arlington. As we watched the wounded being led out of the London Underground following the string of explosions in July, flashbacks to September 11, 2001, were hard to avoid. Like a recurring nightmare, we were forced again to think about our own vulnerabilities here at home.

Most people, when they think about homeland security and the steps that should be taken to protect our country, think about securing our borders, protecting government buildings, and locking cockpit doors. We endure heavy security at airports and border crossings. And even before these recent attacks in London, the attack in Madrid warned us of the need to enhance the security of trains and other transit systems.

But here is something many of us take for granted and don't put under the heading of homeland security: our phone and Internet service. Yet the terrorist attacks on 9/11 and the London attacks showed the stress a crisis places on vital communications infrastructures. Just as many of us couldn't get through on the phone to friends or family in New York or Washington following the attacks there, Londoners on both wireless and land-line phones experienced disruptions as the lines and airwaves were clogged by the spike of traffic and heavy demands of the emergency responders.

September 11 brought home the importance of communications networks during crises. On that day, we saw how ordinary people, held hostage on a doomed aircraft and armed with nothing more than cell phones and amazing courage and determination, managed to do what all the scrambled jets and intelligence operatives could not -- prevent an attack almost certainly aimed at decapitating our government.

Terrorists Target Phones, Web

Now the terrorists are aiming at our economy as well. And America's communications network-- our phones, DSL lines, Wi-Fi connections, and VOIP lines -- make a very attractive target. Homeland Security Secretary Michael Chertoff's recent announcement that he is creating a new assistant secretary for cybersecurity and telecommunications reflects the national-security imperative of ensuring that our nation's information backbone is robust and reliable.

National security traditionally has been thought of as the responsibility of the federal government. Yet, when it comes to telecommunications, much of the responsibility lies in the private sector. According to the U.S. Army War College, approximately 95 percent of the communications critical to our national security run over commercial networks. We know that since the attacks of 9/11, major telecom companies have intensified investment in security and reliability. Yet, continued investment and innovation is needed to stay ahead of the vulnerabilities created by our increasingly networked world.

Interestingly, the consolidation now occurring in the telecom industry may enhance the prospects for reliable communications. Several of the merging companies have pledged to invest significantly to enhance their network and systems. Supporters of these mergers have argued that this level of investment will enable the kind of robustness, technological advances, and effective end-to-end network management that translates *(Continued, Page 14)*

The World of Hacker Conferences

Colleen Hardy, CIP Program

Thirteen years ago, Jeff Moss (a.k.a. Dark Tangent) invited some of his fellow Internet friends to meet in Las Vegas. Moss only knew these people online and wanted a place to meet and discuss cyber related issues, especially hacking. About a hundred people showed up for the first conference in 1992. Thus, Def Con was born.

Def Con has grown into the largest hacker conference in the world and is held in Las Vegas on a yearly basis. Attendees include security professionals, federal officials, IT employees, corporate recruiters, journalists, and intelligence officers. To register for Def Con an attendee pays $80 cash at the door and he or she remains anonymous. An attendee does not have to provide any information to attend.

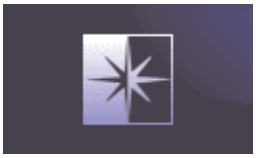
Def Con consists of presentations, demonstrations, and games. Most presentations consist of security experts sharing tips about IT vulnerabilities and how to correct them. Some lectures in this past July's Def Con included: ATM Network Vulnerabilities, Credit Cards: Everything You have Ever Wanted to Know, and Development of an Undergraduate Security Program.

Some of Def Con's main attractions are the games. "Capture the Flag" is the most popular game, consisting of teams of hackers, each breaking into a central server while protecting their own team's resources. "Find the Fed" is another popular game, where the attendees must find a federal official in the crowd and point them out to a conference official. The attendee wins a shirt that says, "I spotted the Fed." The federal official receives a shirt that says, "I am the Fed." Rumor has it that the federal official shirts are coveted.

However, federal agents attend Def Con for more reasons than obtaining a shirt. Federal agents are looking to hire some of the attendees. One federal official stated he was there to learn but also to get names of people that he may be able to call later for help with future cases. Obviously, they will not hire anyone who has performed illegal activity. There is a "Meet the Feds" panel where federal officials and hackers meet face to face. This panel was established to generate greater appreciation and understanding for both sides. It has been estimated that federal officials account for nearly half of the audience at Def Con.

This past July's conference had presentations on how easy it may be to attack supposedly infallible biometric safeguards. There was also a demonstration that radio frequency identification tags could be read from as far away as 69 feet. The demonstrator stated his goal was to raise awareness so that problems can be fixed before they become an issue. Many security professionals at Def Con share that desire. Def Con founder Jeff Moss stated "[p]eople that were considered threats when we started are now considered assets protecting critical infrastructure worldwide." For example, at the 2004 Def Con, three teenagers from Ohio described how they drove around Cincinnati searching for unsecured wireless Internet connections. If they found one, they would ask the people whether they wanted to have their connections fixed. One report published by CERT at Carnegie Mellon University estimated that thousands of weaknesses are discovered in major software products every year, many of them by the people who attend Def Con.

In 1997 Def Con creator, Jeff Moss created the Black Hat conference. Black Hat is tailored more towards a corporate and federal agency audience. Black Hat is also held in Las Vegas and precedes Def Con. Black Hat is a lot more pricey than Def Con, costing at least a *(Continued, Page 15)*



National Policy Forum

Terrorism, Security and America's Purpose: Towards a More Comprehensive Strategy

Maeve Dion, CIP Program

The New America Foundation (NAF) held this forum on Sept. 6-7, in Washington, D.C. The forum addressed five main themes - "underlying causes of global terrorism, strategies to confront terrorism, U.S. grand strategy, national security and civil liberties, and the promotion of democracy and human rights." The conference sought "to encourage open and critical thinking about U.S. foreign policies generally, and counter-terrorism specifically, and to build consensus for strategies that effectively fight terrorism in accordance with core American values."

In the months preceding the forum, NAF convened five working groups composed of professionals from both the public and private sectors. Within each working group, three members were asked to present papers aligned with the themes of the working groups and designed to provoke discussion in advance of the policy forum. These discussions were held online in private working group blogs. Suzanne Spaulding, chair of the Homeland Security and Freedom Working Group, invited John McCarthy to draft a paper on critical infrastructure protection and its relationship to homeland security and freedom. McCarthy also monitored the online discussion and participated in the working group session held during the first day of the policy forum.

This working group debated various subjects, including (1) the need for a "comprehensive national strategy [for protecting homeland security] that ... gives adequate attention to the role of the private sector and economic factors, sets forth clear goals and objectives, and provides a solid basis for establishing priorities and allocating resources" in accordance with a risk management plan; (2) the state of U.S. capabilities for responding to catastrophic events; (3) the importance of "protect[ing] privacy and due process while strengthening government's information awareness;" and (4) the adequacy of existing legal structures given the long-term threat of terrorism and current U.S. policy. Each working group produced a summary paper, and those summaries and the working group draft papers are available at http://www.americaspurpose.org/.

In addition to the working groups, more than 65 other eminent professionals spoke in panels or individually at the policy forum, including Rt. Hon. Kim Campbell, Hon. Madeleine K. Albright, Hon. Juan Zarate, Daniel Levy, Hon. Jane Harman, George Soros, General Wesley Clark, Hon. Chuck Hagel, Hon. James Steinberg, Yosri Fouda, Hon. Lawrence Korb, Rita E. Hauser, Juliette Kayyem, Hon. Joseph Biden, Gerold Yonas, Grover Norquist, Brigadier General James Cullen (U.S. Army, ret.), and Hon. John Ashcroft.

At the conclusion of the forum, a bipartisan group of national leaders (organized by the Partnership for a Secure America, co-chaired by former U.S. Sen. Warren Rudman and former U.S. Rep. Lee Hamilton) issued "a statement of principles to guide the next-phase approach to dealing with America's and the world's security challenges." The principles are available at http://www.psaonline.org/public_statements.html.

A video archive of the policy forum is available at http://www.americaspurpose.org/. ❖

McCarthy *(Cont. from Page 11)* into critical national-security benefits.

These types of combined networks also could facilitate coordination and promote efficiencies vital to preventing, mitigating, and responding to disruptions and attacks. Since the breakup of Ma Bell in the mid-'80s, telecom professionals have quietly put aside their business differences at the National Communications Center, an organization that attempts to coordinate responses to infrastructure disruptions across the nation.

U.S. Demands Reliable Response

Having a single company control a larger portion of our increasingly complex communications infrastructure can facilitate this type of effort. Since companies have been fearful of sharing sensitive network mapping information with the government or each other, combining significant pieces of these networks under a single management structure may be the best practical way to better identify vulnerabilities and develop essential "work-arounds" to deal with disruptions to parts of the system. A single entity managing a broader piece of the network can ensure effective redundancies at critical points in the system.

Our national security depends on a reliable and robust worldwide communications infrastructure. It is vital to essential government functions, fundamental to virtually every aspect of our economy, and an integral part of our everyday lives. In a time of crisis, such as following a terrorist attack, the single most important element in managing our national response -- the response of government, business, and the public -- will be ensuring effective communications capabilities. ❖

John McCarthy is the director and principal investigator of the Critical Infrastructure Protection Program at George Mason University.

Institute for Information Infrastructure Protection

The Institute for Information Infrastructure Protection (The I3P) is a Consortium that includes academic institutions, federally-funded labs and nonprofit organizations. With a nationwide membership that continues to grow, the I3P brings experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.

The I3P functions as a virtual national lab with the ability to organize teams and workgroups to address research and policy-related aspects of the vulnerabilities inherent in the information infrastructure. The I3P is managed by Dartmouth College.

The Mission Tasks of I3P include:

- Collaborate with academia, industry and government to develop a national R&D agenda for cyber security;
- Serve as an information clearinghouse on the status of R&D efforts for information infrastructure protection;
- Foster collaboration among cyber security R&D efforts in academia, industry and government; and
- Facilitate specific high leverage research and the development of new security technology for information infrastructure protection.

Hacker Conferences *(Cont. from Page 12)* thousand dollars to attend. Moss' goal was to bring together the best minds of the computer underground with the leading security professionals. Black Hat also hosts conferences in Singapore, Tokyo, and Amsterdam.

Black Hat consists of presentations and seminars demonstrating new and exclusive research. This past July, one demonstration caused a lot of commotion. Michael Lynn, a former employee of Internet Security Systems Inc. gave a presentation illustrating the flaws in Cisco Systems Inc.'s Internetwork Operating System. Cisco obtained an injunction to stop all future presentations and prevent the release of related information. However, the material can easily be found on the Internet.

Some people attend both Black Hat and Def Con. Vaughn Hendricks, a systems integrator of Lockheed Martin Missions Systems, attended both conferences in 2000 and stated, "Black Hat/Def Con offers a unique opportunity for collaboration between good guys and bad guys. I can listen to premiere network security gurus and ex-hackers and discuss vulnerabilities in depth."

Blue Hat

Microsoft is also realizing that hackers may be a useful business tool. They recently held a meeting with hackers (called "security researchers" for this event) to watch how exploits are run against the Windows operating system. Within minutes, the hackers were able to find targets and exploit the machines.

Microsoft's goal for the conference was to learn about some of their vulnerabilities. The security researchers were grateful to help Microsoft. One researcher stated that it was rare to present to the people who are both responsible for and capable of correcting the issues that he finds.

After this initial meeting, Microsoft is strongly considering holding these meetings twice a year. Stephen Toulouse, a program manager in Microsoft's security unit, said Microsoft is becoming more comfortable getting into face-to-face interactions with security researchers. Toulouse stated the purpose of the Blue Hat conference is to help make Microsoft's product line as a whole more secure. The two day event is titled Blue Hat because of the blue badges Microsoft employees wear. ❖

Emergency Management Institute *(Cont. from Page 6)* Training Center (NETC) in Emmitsburg, Maryland. The campus is located 12 miles south of Gettysburg, Pennsylvania, 75 miles north of Washington, DC, and 50 miles northwest of Baltimore, Maryland.

The 107-acre campus is shared by the United States Fire Administration (USFA), the National Fire Academy (NFA), the Emergency Management Institute (EMI), the Field Personnel Operations Division, and the Satellite Procurement Office. All these components are part of FEMA, one of the four directorates in DHS. The NETC campus has fully equipped air-conditioned classrooms, lodging for students, a Learning Resource Center, and dining and recreational facilities. There also are several specialized facilities, such as the Simulation and Exercise Lab, a television studio (EENET), and two computer laboratories that are integral to the instruction of many courses. ❖

CERT *(Continued from Page 5)* Protecting critical infrastructures is a challenge. One way to meet that challenge is to build a community of practitioners with knowledge in depth who have the skills and knowledge to protect networks, respond to compromises, and perform forensics effectively. ❖

George Mason University's Biodefense Program: A Student Perspective

Colleen Hardy, CIP Program

George Mason University established its Biodefense Degree program in the fall of 2003. The main objective of the program is to prepare students for a career in the area of biodefense including academia, industry, and government. The biodefense program was designed to empower George Mason students with critical knowledge and vital skills to become an asset to national security. The program is affiliated with the George Mason University National Center for Biodefense & Infectious Diseases and offers both an MS and a PhD in Biodefense, as well as certificate programs.

I am currently a doctoral student at George Mason University's biodefense program. I have thoroughly enjoyed the classes and have learned a great deal. Over the past year I have taken the required core courses. The core classes include:

- Introduction to Biodefense /Threat Analysis I: Bacterial Agents
- Introduction to Biodefense/Threat Analysis II: Viral Agents
- Introduction to Biodefense/Threat Analysis III: Toxins
- Crisis and Consequence Management

This past summer I took a course called Weapons of Mass Destruction (WMD) Incidence Response. Course exemplified the aftermath of a WMD attack. The course included a class project to plan a terrorist attack. The class was broken into five groups and each group was assigned a weapon of mass destruction: chemical, biological, nuclear, radiological, or explosive. I was in the radiological group and found it to be an extremely eye-opening experience. There was a large amount of planning and surveillance required; however, planning a terrorist attack was easier than I had anticipated. This class was an excellent illustration of the different threats we face daily and how the United States is prepared to handle the consequences of a WMD attack.

The biodefense program offers unique courses on critical national security topics. For example, there are scientific courses, such as "Dispersal Patterns of Biological Agents." Medical courses include "Approaches to BW Medical Treatment and Response." There are also courses on counterterrorism issues such as "Examining Terrorist Groups" and "Counter-Terrorism and Civil Rights." The distinctive courses offered, combined with the extremely accomplished faculty, make the biodefense program a great asset to the future of national security. ❖

Legal Insights *(Cont. from Page 8)* training of technology and policy experts. But ethics considerations recall the larger view of education defined as "critical," but not "critical infrastructure." The teaching of values and ethics is a broad aspect of education, and one which applies to all things taught, regardless of their relationship to critical infrastructure.

Regardless of the outcome of an examination of this issue, it is beyond dispute that education is an indispensable requirement for a functioning democracy. Without it, society would collapse. Furthermore, education has a specific and immediate role to play in the development of critical infrastructure protection in both the cyber and physical spheres. Although "critical," perhaps education as a "critical infrastructure" is limited to those specific and immediate roles. In any event, both the critical and the critical infrastructure aspects of the US public education system have important roles to play. Policy makers must remember education's role in the overall security, both short and long-term, of the nation. ❖

[1] Robert Lemos, Report: Cost of phishing not so high, News.com 1, (December 1, 2004), at http://news.com.com/Report+Cost+of+phishing+not+so+high/2100-7349_3-5473170.html.

[2] Sean Michael Kerner, The Cost of Phishing Hits $1.2 Billion, Ecommerce 2 (May 6, 2004), at http://www.internetnews.com/ec-news/article.php/3350891.

[3] See Aaron Emigh, Anti-Phishing Technology (January 19, 2005), at https://antiphishing.kavi.com/events/Conference_Notes/phishing-sfectf-report.pdf.

CHDS *(Cont. from Page 3)* One major consequence of this finding is that the traditional classroom is under pressure to provide prospective, intra-student interaction, and workshop or discussion modes of learning. Students want to know what the instructor thinks, or how to solve a problem rather than listen to a lecture that can better be presented by technology.

We use Microsoft PowerPoint as an authoring tool. Instructors are encouraged to prepare short lecture modules (15-20 slides) along with text annotation that can be recorded in audio format for further polishing and conversion to flash media by our web development team. Once these lectures are cleaned up and the audio synchronized with the visual elements (text, pictures, animations), it is converted and embedded in QuickTime "wrappers" so it can be delivered via the Web or DVD. These modules are then incorporated into the course using the open source learning management system, Moodle.

Audio lectures (text, articles, readings) are similarly cleaned up and packaged as short clips and downloaded into iTunes. Students can then easily load the audio tracks into their iPODs for playback. In some cases, students use iTalk (microphone attachment to the iPOD) to further annotate the audio tracks.

Partnerships

CHDS recognizes that this approach is time-consuming and expensive. Therefore, DHS has authorized a limited number of partnerships so that the curriculum and associated online content can be shared with other universities. Currently, the University of Washington, University of Connecticut, and several smaller universities have transferred parts of the CHDS degree program into their own homeland security programs. These partners have full access to the content developed by CHDS under a reciprocal agreement. If you are interested in partnering, please contact the authors. ❖

Ted Lewis can be reached at tlewis@nps.edu and Rudy Darken can be reached at darken@nps.navy.mil.

For more information on CIP Practitioner Training and Education....

The **National Memorial Institute for the Prevention of Terrorism**, based in Oklahoma City, maintains a national listing of training courses and other information for First Responders, Health Care Providers and others on Terrorism Preparedness and Response including WMD training and sustainment, disaster recovery, plans, bioterrorism, chemical terrorism, radiological terrorism, among others. The list includes university, public, and government training. It can be accessed at: http://www.mipt.org/ trainingcourses.asp.

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 infrastructure. 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/cgi-bin/wa?SUBED1=cipp-report-l&A=1