THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 7 NUMBER 12

JUNE 2009

EDUCATION AND TRAINING

Contact: CIPP02@gmu.edu
703.993.4840

Click **here** to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

The June issue of The CIP Report highlights domestic and international education and training programs that incorporate the complex issues of critical infrastructure and key resources protection into their curriculum.

The George Mason University School of Public Policy provides information about the development of a new graduate degree program. This degree, the Executive Masters in Public Policy: Leadership in Critical Infrastructure Protection (EMPP-CIP), was created through the partnership between School of Public Policy and the Center for Infrastructure Protection. They also provide information about the Federal Emergency Management Agency (FEMA) cooperative agreement that was recently awarded to them and the Center for Infrastructure Protection.

We are pleased to include information about new and revised courses and training programs offered through the Department of Homeland Security (DHS) Office of Infrastructure Protection. These professional programs are available to Federal homeland security professionals as well as to private sector professionals who wish to enhance their knowledge of critical infrastructure and information protection. In addition to George Mason and the DHS Office of Infrastructure Protection, there are a number of innovative universities and training academies that have integrated critical infrastructure issues and topics into their programs. We are delighted to feature both domestic and international education and training programs in this issue.

The Legal Insights column this month reveals the development of a new law concentration offered through the George Mason University School of Law. The Homeland and National Security Law Concentration in the Juris Doctor program prepares students for careers in homeland and national security in both the public and private sector. The Cyber Conflict Perspectives monthly column proposes an ideal curriculum for international cyber incident management legal studies. Finally, this issue includes information about the upcoming 3rd National Conference on Security Analysis and Risk Management that the Center for Infrastructure Protection is co-hosting.

We hope you enjoy this issue of The CIP Report as well as find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP
George Mason University, School of Law

Graduate Concentration in Leadership for Critical Infrastructure Protection Combining Academic Excellence and Professional Development

by Christine Pommerening, Research Assistant Professor
George Mason University School of Public Policy

Educational Vision

The Executive Masters in Public Policy: Leadership in Critical Infrastructure Protection (EMPP-CIP) is currently under development at George Mason University, a joint effort by the School of Public Policy and the School of Law's Center for Infrastructure Protection.

With its focus on developing leaders in critical infrastructure protection, this new EMPP-CIP degree is unique in combining academic excellence and professional development. As such, it also fits into the National Infrastructure Protection Plan education strategy, which views the role of university programs as presenting advanced knowledge, research, and theories to promote professional development for the protection of critical infrastructure and key resources.

While most people in the homeland security community agree that we indeed need a robust and comprehensive set of courses and degrees in all facets of the field, turning such visions into practice is where the rubber meets the road.

Turning Vision into Practice

Typically, the demand from prospective students (and their current and future employers) starts out at a different level than the supply of courses offered by academic institutions. Emerging fields of study such as CIP do not yet have a well-defined place within the traditional disciplines — they are too broad and too new to easily fit within academic accreditation and approval standards established to ensure consistent quality. Even if they were not subject to accreditation and approval, graduate schools and their faculty cannot compromise on the quality and rigor of their base curriculum.

Thus, the approach here is to adapt an established master's curriculum for a particular audience. This guarantees academic excellence by providing a solid foundation rather than starting from scratch or offering a patchwork of unrelated courses. At the same time, it validates the subject-matter expertise and job experience of students dealing with CIP issues. Through this combination, the level of knowledge and thought leadership is elevated in both academia and the workplace.

In addition to the School of Public Policy's EMPP-CIP degree, George Mason University's School of Law is also launching a new concentration in Homeland and National Security Law (see page 6).

Program Practice

The goal of the EMPP-CIP is to develop and advance professionals within and across governmental agencies, non-governmental organizations, and the private sector that deal with critical infrastructure risk management. Participants from these organizations will meet one another, develop professional relationships, share their unique perspectives, and come to understand one another's organizational exigencies. The program cultivates strategic thinking and analytical capabilities concerning risks and resilience in various areas, resulting in an ability to exercise leadership within and beyond each student's organization.

Applicants must be a GS-12 or its private sector equivalent and must be sponsored by their employers, which will certify experience level. Each select group of 20-25 professionals will move through the program as a cohort in an 18-month period of intensive study, occurring primarily on Fridays and

(Continued on Page 15)

Mason Receives FEMA Grant to Teach Infrastructure Protection

by Brien Benson, Ph.D.
Program Director, Enterprise Risk Management Training Program
Research Professor, George Mason University School of Public Policy

George Mason University was recently awarded a $3.5 million cooperative agreement by the Federal Emergency Management Agency (FEMA) to develop training in infrastructure protection. The instruction is directed at the electric power industry and will show how the use of enterprise risk management techniques can help insure infrastructure protection. The project is a partnership of George Mason's School of Public Policy and the Law School's Center for Infrastructure Protection.

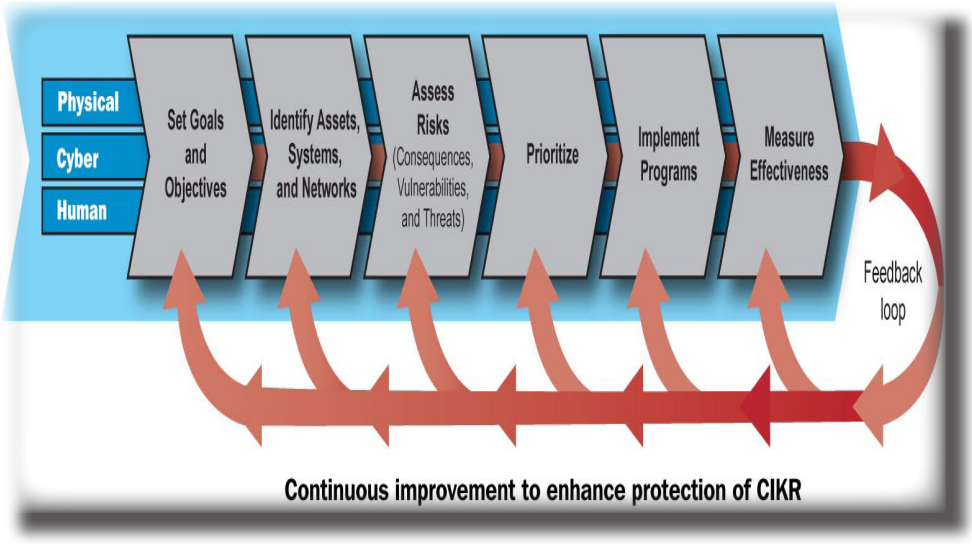
Enterprise risk management (ERM) is a management tool developed in the 1960s to help firms deal with the increasing complexity of risks arising from the merger wave of the period. At first ERM was exclusively a financial tool, but it has spread to include operations, marketing and strategic planning. ERM has gained widespread acceptance in the business community, and it is the subject of numerous professional articles and books.

In awarding this cooperative agreement to George Mason University, FEMA seeks to use a widely accepted business tool as a means to develop more sophisticated planning for and management of critical infrastructure protection. One major goal of the training is to improve coordination between industry and government officials at the state and local level, in particular regulatory officials and state officials charged with overall responsibility for energy security and continuity. Training sessions will bring together public- and private-sector professionals in order to encourage increased understanding of each other's perspectives.

Another important goal of the training is to help achieve commonality of language regarding risk. At present, words like 'risk,' 'hazard,' 'resiliency,' and 'accident' are used to mean widely different things, leading to confusion in communication. One effort to address this problem is the Department of Homeland Security's 50-page booklet "Risk Steering Committee: DHS Risk Lexicon," which sets out formal definitions of many terms currently used loosely with divergent meanings. The George Mason training will encourage participants to develop a more common understanding of words frequently used in discussing risk management.

Instructional material developed under FEMA's Competitive Training Grants Program must undergo a rigorous review process, in which outside subject matter experts review the proposed training modules and then negotiate changes with the grantee. Once the training material is approved by DHS, George Mason will begin the Delivery Phase of the agreement, in which training will be conducted broadly throughout the nation. George Mason will work in close cooperation with the Edison Electric Institute and the other major electric power trade

(Continued on Page 17)



DHS Launches New Course on CIKR Support Annex

by DHS Office of Infrastructure Protection

The Department of Homeland Security's Office of Infrastructure Protection has launched a new independent study course that focuses on how protection of national critical infrastructure and key resources (CIKR) is integrated into the National Response Framework (NRF). The NRF is the nation's blueprint for responding to terrorist incidents or natural disasters.

The CIKR Support Annex training (IS-821) presents the policies, procedures, and mechanisms used by the many public and private sector entities responsible for assessing, prioritizing, protecting, and restoring the nation's critical infrastructure during the response to natural disasters or terrorist attacks.

The CIKR Support Annex is essentially the bridge linking "steady-state" CIKR protection as detailed in the National Infrastructure Protection Plan (NIPP) and the NRF's unified approach to domestic incident management. The training is available free of charge at http://training.fema.gov/emiweb/is/is821.asp.

CIKR Webinars

The Office of Infrastructure Protection also offers free Webinars about CIKR and related subjects. Read more about this on page 7.

The CIKR Support Annex online course describes:

- The relationship between the National Response Framework and CIKR prevention, protection, and response and recovery;
- The role of the Infrastructure Liaison in supporting coordination with the CIKR sectors and all levels of partners; and
- NRF processes for integrating CIKR considerations into incident response.

The CIKR Support Annex course is an introductory course intended for a broad audience, including Federal homeland security professionals and Tribal, State, local, and private sector professionals from such fields as emergency management, infrastructure protection, planning, and security.

Participants who take IS-821 receive 0.1 CEU credit. IS-800.B on the National Response Framework is a prerequisite, and IS-860 on the National Infrastructure Protection Plan also should be taken prior to the support annex course. ❖

More information about the NRF and other NRF-related training is available at www.fema.gov/nrf.

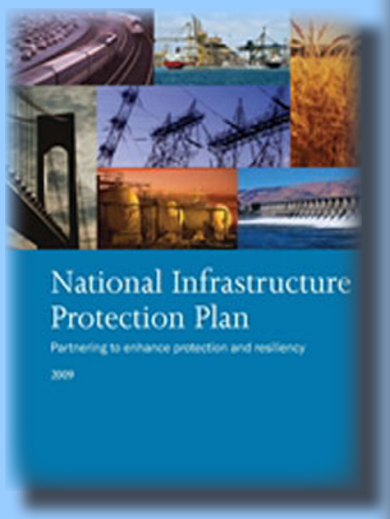
More information on the NIPP and CIKR is available at www.dhs.gov/nipp.

No Cost Infrastructure Protection Training Available

by DHS Office of Infrastructure Protection

DHS announced the release of a revised version of *IS-860.a National Infrastructure Protection Plan (NIPP)*. This online course was jointly developed by the DHS Office of Infrastructure Protection and FEMA's Emergency Management Institute. *IS-860.a* highlights:

- Explains the importance of protecting critical infrastructure and key resources (CIKR);
- Identifies the relevant authorities and roles for CIKR protection efforts;
- Provides an overview of the NIPP unifying structure for the integration of CIKR protection efforts — including the sector security partnership model, the risk management framework, and the information sharing process; and
- Covers changes and enhancements to the 2009 NIPP update, including the addition of the 18th CIKR sector (Critical Manufacturing), the role of the Regional Consortium Coordinating Council, and other elements of the new program.



The NIPP, originally released in 2006, was revised and updated early this year to reflect experience and changes in the threat environment.

The free course is available on FEMA's Emergency Management Institute learning site, accessible at www.dhs.gov/nipp. The course requires about two hours to complete, and provides 0.2 CEU to those passing the 25-question final exam. Individuals who have successfully completed IS-860 need not take the updated course; however, IS-860.a may serve as a useful refresher or primer on the 2009 updates. ❖

Contact Information: Ron Eschmann, DHS Office of Infrastructure Protection, Partnership and Outreach Division, (703) 235-3666 / ron.eschmann@hq.dhs.gov

Legal Insights

George Mason Introduces New Homeland and National Security Law Concentration

The George Mason University School of Law has approved a new specialty concentration in Homeland and National Security Law, enabling students to present potential employers, both in government and the private sector, with credentials reflecting a solid foundation in homeland and national security law.

This new concentration is an example of Mason Law's innovation and proactive efforts to produce future generations of law professionals who are focused and dedicated to our homeland security.

Mason is one of just two law schools in the United States with a homeland security focus to its national security curriculum. Recent years have seen a growing interest — among scholars, students, government officials, and private practitioners alike — in the fields of national security law, homeland security law, international law, and related topics.

While some law schools offer a course or two in security-related topics, such as 'terrorism and national security' or 'domestic preparedness law,' Mason Law's new specialty concentration in Homeland and National Security Law uniquely enables students to focus on the 'homeland' aspect of national security. Topics to be covered include legal aspects of cyber security and the protection of other critical infrastructure, border control, disaster preparedness and response, and intelligence and information sharing.

Mason Law is uniquely positioned to develop this curriculum. George Mason has four tenured and tenure-track faculty who teach in these fields (Jonathan Mitchell, Jeremy Rabkin, Neomi Rao, and Nathan Sales). These professors have worked in the homeland security profession before joining Mason. The law school also has numerous adjunct faculty who currently work in the homeland security fields, as well as those who have past experience in the area.

Also, the law school's close relationship with the Center for Infrastructure Protection offers opportunities to supplement Mason's in-house expertise with outside and affiliated experts and research projects in homeland and national security law.

Specialty concentrations provide students with expertise in a particular substantive area, but also flexibility in terms of taking electives on a broad range of topics. Generally, in order to complete a concentration, a student must complete 14 to 16 credit hours in that subject area. The new Homeland and National Security Law Concentration requires students to take six courses: Homeland Security Law, National Security Law, and Administrative Law, plus three elective courses selected from a list of relevant homeland security courses, such as technology and terrorism, immigration law, international law, aviation law, and privacy law.

The addition of the new concentration brings to 11 the number of concentrations available to George Mason Law students. The other ten concentrations are in Corporate and Securities Law, Criminal Law, Intellectual Property Law, International Business Law, Legal and Economic Theory, Litigation Law, Personal Law, Regulatory Law, Tax Law, and Technology Law. ❖

Click here for more information on the Homeland and National Security Law Concentration, and for information on School of Law go to http://www.law.gmu.edu/.

Office of Infrastructure Protection Continues Successful Critical Infrastructure and Key Resources Learning Series

by DHS Office of Infrastructure Protection

More than 250 public- and private-sector partners participated in the April 2009 offering of the Department of Homeland Security's 2009 Critical Infrastructure and Key Resources (CIKR) Learning Series. Participants discovered how engaged partnerships benefit both public and private sectors during a disaster. Presented by R. James Caverly, Director of the Office of Infrastructure Protection's Partnership and Outreach Division, the most recent seminar closely examined the roadmap for integrating critical infrastructure response into a unified approach to incident management.

The Office of Infrastructure Protection sponsors these one-hour Webinars on issues of interest to government stakeholders and owners and operators of the nation's CIKR. The Series provides the latest information on infrastructure protection tools, trends, issues, and best practices.

Upcoming CIKR Learning Series Webinar

2009 Hurricane Season: A Readiness Guide for Critical Infrastructure Partners

23 June 2009
2:00 PM - 3:00 PM(ET)

More than 3,000 people have participated in the CIKR Learning Series since its initial offering in August 2008. Topics covered include: Improvised Explosive Devices; The Role of Regional Coalitions in Implementing the National Infrastructure Protection Plan; Critical Infrastructure Protection Mission and Vision; and The Effective Use and Visualization of CIKR Data.

Information provided in these Webinars is helpful to a wide range of security partners, including emergency management professionals and systems, security, facilities, operations, and financial or risk managers — anyone engaged in activities promoting infrastructure protection and resilience. ❖

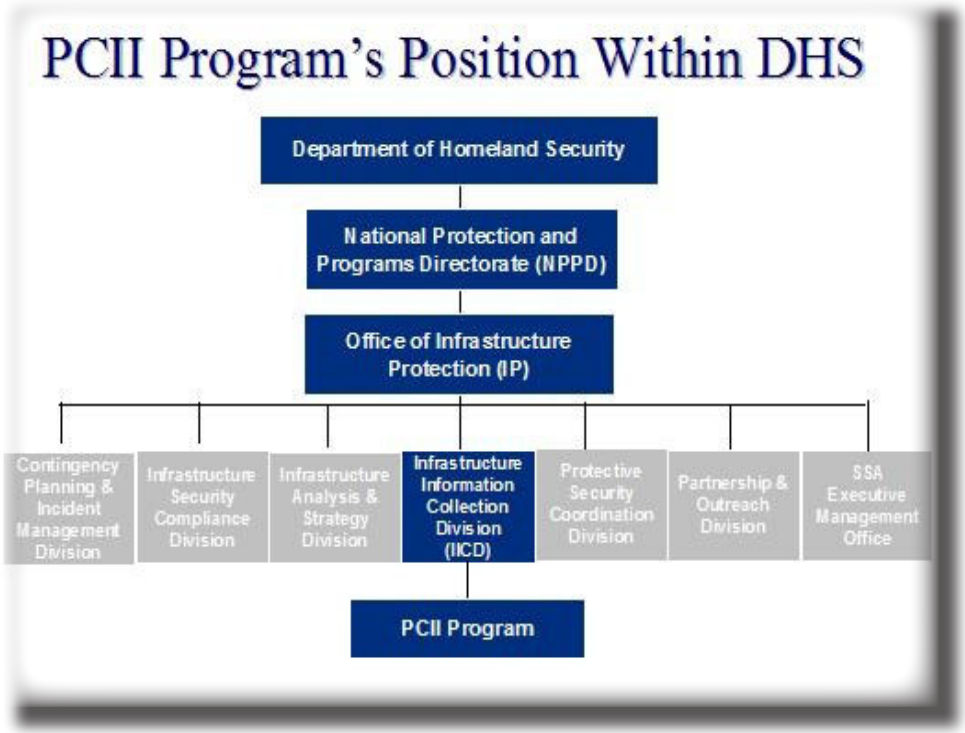
To view the previously recorded Webinar "Engaged Partnership for Disaster Response," visit https://connect.hsin.gov/p21834718/.

To register for notification of future CIKR Learning Series Webinars, please visit the program's Web page at http://www.dhs.gov/xprevprot/programs/gc_1231165582452.shtm.

PCII Program Procedures Manual

by Laura L.S. Kimberly, PCII Program Manager
IICD/IP/NPPD
Department of Homeland Security

The Department of Homeland Security's Protected Critical Infrastructure Information (PCII) Program Office is pleased to announce that a new edition of the PCII Program Procedures Manual is now available. A copy of the 2009 Manual can be downloaded here. The updated Manual reflects changes made to PCII Program policies, procedures and requirements pursuant to the issuance of the Final Rule and additional operational experience gained since 2005.



Information validated as PCII is protected from public disclosure under the Freedom of Information Act (FOIA) and similar State and local disclosure laws, and from use in civil litigation. As owners/operators of critical infrastructure, your participation in information-sharing partnerships and the PCII Program is important. The Manual will help you understand how to submit information and how it is safeguarded and handled once it is validated as PCII.

In addition to clarifying the policies and procedures governing the receipt, validation, handling, storage, marking and use of PCII, the Manual highlights the following policies:

Enhanced oversight:

Enhanced oversight ensures that PCII is only accessed by authorized and trained individuals with a need to know, and that PCII is used appropriately for homeland security purposes to analyze threats and vulnerabilities.

Stricter requirements for a change in status:

The Manual refines guidance on the limited circumstances in which validated information relinquishes its protected status.

Clarification of what information is PCII protected:

Only critical infrastructure information (CII) that is received, validated and marked by DHS as PCII is protected by the Critical Infrastructure Information Act of 2002 (CII Act). When validated and marked information is subsequently shared with accredited government entities and authorized users, the protections of the CII Act apply. Unmarked and invalidated CII retained by the submitter does

(Continued on Page 17)

DHS Releases Executive Training on Use of Protected Critical Infrastructure Information

by DHS Protected Critical Infrastructure Information (PCII) Program

The Department of Homeland Security's Protected Critical Infrastructure Information (PCII) Program protects critical infrastructure information from public disclosure while allowing the information to be shared with government security analysts. The PCII Program Office is pleased to announce the release of a new online Authorized PCII User Training created specifically for senior executives.

Advent of the new administration in January 2009 brought many new people to the PCII Program, some of whom need to become versant in PCII handling as quickly as possible. The executive training module provides a brief, high-level introduction to the policies and procedures surrounding the use, dissemination, and handling of PCII. Busy executives will gain a workable understanding of the basics of the PCII Program in about 15 minutes, including an overview of the basics of PCII safeguarding policies and a brief question and answer session at the end of the course.

The new course is only available to senior executives whose responsibilities merit a concise overview of the Program (as opposed to the standard Web-based Authorized User Training, which is longer and more detailed).

PCII Authorized User Training is an essential part of the process that security analysts go through to gain access to PCII. Participants in the PCII Program must be government employees or government contractors, have specific homeland security duties, complete the version of PCII Authorized User Training appropriate to their job responsibilities, and have a specific need to know the particular information to be accessed. ❖

To learn more about training offered by the PCII Program Office or about the Program in general, please e-mail PCII-info@dhs.gov, call (202) 360-3023, or visit the PCII Web page at http://www.dhs.gov/PCII.

CAPTAP
Popular DHS Training and Technical Assistance for State and Local CIP

by DHS Office of Infrastructure Protection

To support those on the front lines protecting the nation's critical infrastructure and key resources (CIKR), the Department of Homeland Security Office of Infrastructure Protection (DHS/IP) offers free training on critical infrastructure protection and planning to federal, state, and local first responders, emergency managers, and homeland security officials. Known as the CIKR Asset Protection Technical Assistance Program, or CAPTAP, the training is offered in partnership with the DHS Federal Emergency Management Agency and is conducted by National Guard instructors.

CAPTAP trains participants on how to identify and prioritize CIKR, conduct infrastructure vulnerability assessments, and build public and private partnerships to support their jurisdiction's infrastructure protection process.

Training on IP's Systems and Tools

Since 2005, CAPTAP has trained more than 2,500 participants. In addition to an overview of critical infrastructure protection (CIP), CAPTAP provides information on how to establish CIP programs, and discusses the benefits of Protected Critical Infrastructure Information (PCII), an information-protection program that enhances information sharing between the private sector and the government.

WV National Guardsman First Sergeant Dan Phillips leads CAPTAP training course.

CAPTAP training includes hands-on experience using the Constellation/Automated Critical Asset Management System (C/ACAMS) — a Web-based data collection and management tool. C/ACAMS provides methods for cataloguing infrastructure sites and systems and includes instruction on how to create Buffer Zone Plans and prioritize assets. C/ACAMS also provides access to vulnerability assessment tools and can be tailored to the needs of individual jurisdictions, allowing users to determine the appropriate level of detail and to create customized reports.

Another feature of CAPTAP is an overview of Integrated Common Analytical Viewer (iCAV) mapping functions within C/ACAMS. The iCAV application allows users to visualize infrastructure geospatially for increased situational awareness.

In response to stakeholder requests for expanded training options, DHS IP is upgrading CAPTAP training to include a Web-based component to teach C/ACAMS functions using interactive lessons and knowledge check points. Web-based training will reduce the amount of time and resources needed for state participation in CAPTAP.

National CAPTAP Conference

Earlier this year, CAPTAP held its first national training conference, bringing together nearly 200 representatives from federal agencies, 38 states, two territories, and other local government representatives for a two-day discussion on how to protect vital infrastructure and establish CIP programs. Participants exchanged tips on best practices and lessons learned, while sharing insights on current CIKR protection tools

(Continued on Page 17)

Critical Infrastructure Protection Education and Training Programs

The mission of critical infrastructure protection (CIP) requires a robust education and training community. Today there are a variety of domestic and international programs that have developed, or are currently developing, curricula that include the examination of critical infrastructure protection. The following list provides a sample of existing CIP degrees, concentrations, courses, and training programs.

Graduate Degree

Master in Strategic Planning for Critical Infrastructures (MSPCI)
The University of Washington College of Built Environments, Department of Urban Design and Planning

The Master in Strategic Planning for Critical Infrastructures is a fully accredited online graduate program that commences each fall. Students "learn to apply strategic planning and decision-making strategies to analyze the vulnerabilities of critical infrastructures; plan responses to failures; and develop resilience." The degree blends education in strategic planning and systems theory, and includes topics such as communications and the legal and ethical issues relevant to homeland security.

In addition to the MSPCI degree, the Department of Urban Design and Planning collaborates with the School of Public Health to develop courses that instruct students about public health and emergency response systems.

For more information about the MSPCI degree, please visit the following website: http://www.outreach.washington.edu/mspci/.

Graduate Concentration

Specialty: *Critical Infrastructure Protection*
Master of Science in Computer Science
Missouri University of Science and Technology

This specialty provides computer science students with an opportunity to specialize in critical infrastructure protection, focusing on vital integrated systems of the nation's critical infrastructures. The intent of this program is to "improve the quality, survivability, security, and reliability of critical systems using the broadest-based technology possible, to grow a workforce aware of and trained in security (physical and cyber), and to stimulate the economic viability of U.S. corporations and institutions by improving the security, reliability, and survivability of their critical infrastructures."

> ***"Missouri S&T's strong emphasis in science and engineering allows us to conduct research and educate students in critical cyber-physical infrastructure protection."***
>
> — Dr. Bruce McMillin, Professor and Graduate Coordinator
> Director of Center for Information Assurance
> Department of Computer Science, Missouri University of Science and Technology

For more information about this program, please visit the following website: http://cs.mst.edu/graduatedegreeprograms/mscomputerscience.html.

Individual Courses

Graduate Course: *Critical Infrastructure Protection of Health Care Delivery Systems*
Master of Homeland Security in Public Health Preparedness
The Pennsylvania State University

Critical Infrastructure Protection of Health Care Delivery Systems examines the operations of health care delivery systems during a natural disaster or terrorist attack, including the disaster's effects on "transport systems, computer and internet security, communications, energy supply, and industry and governmental institutions." The students study the consequences of

(Continued on Page 12)

CIP *(Cont. from 11)*

the disruption of health care delivery systems.

The course is part of the curriculum for the Master of Homeland Security in Public Health Preparedness, an online graduate degree program developed by the Penn State College of Medicine. This program is currently the sole homeland security degree offered by a medical school in the United States. The course is also required for Penn State's online Graduate Certificate in Bioterrorism Preparedness and the online Graduate Certificate in Disaster Preparedness.

For more information about the course and these programs, please visit the following website: http://www.worldcampus.psu.edu/MasterinHomelandSecurity.shtml.

Graduate Course: *Protecting Critical Resources and Infrastructure*
The University of Texas at Dallas School of Economic, Political and Policy Sciences

The *Protecting Critical Resources and Infrastructure* course instructs students about the methods, policies, plans, and innovative technologies that are currently involved in protecting both public and private critical resources and infrastructure. This course requires students to learn various theories of how to respond to threats to infrastructure and assets, as well as how to apply preventative and mitigation measures.

"I believe that homeland security courses such as UT Dallas' Protecting Critical Resources and Infrastructure course are more important than ever to Public Affairs students who will eventually manage organizations that have large amounts of resources and assets that need to be protected from external and internal threats."

— Dr. Nicolas A. Valcik, Associate Director of the Office of Strategic Planning and Analysis and Clinical Assistant Professor Program of Public Affairs, The University of Texas at Dallas

This course is a core requirement for the Graduate Certificate in Homeland Security offered through the Public Affairs Program. In addition, this course may apply towards the Master of Public Affairs, the Master of Science in Criminology, or the Master of Science in International Political Economy.

For more information about this course and the programs offered within the School of Economic, Political and Policy Sciences, please visit the following website: http://epps.utdallas.edu/.

Certificate Course: *Information Assurance and Critical Infrastructure Protection*
Information Assurance Program National Defense University Information Resources Management College

The *Information Assurance and Critical Infrastructure Protection* course focuses on public policy and strategic management. Students will "analyze laws, national strategies, and public policies; and assess the strengths and weaknesses of various approaches for assuring the confidentiality, integrity, and availability of those information assets created, stored, processed, and communicated by information systems and critical information infrastructures."

The course is part of the Information Assurance (IA) Program, which consists of a variety of certificates for information systems security professionals, senior systems managers, risk analysts, and chief information security officers.

For more information about the course and program, please visit the following website: http://www.ndu.edu/irmc/index.htm.

<u>International Training Programs</u>

Protecting Critical Infrastructure Program
ARC Training International Academy for Security Management United Kingdom

The Protecting Critical Infrastructure Program is a five-day training program for security managers who exercise leadership roles in the critical infrastructure

(Continued on Page 16)

Cyber Conflict Perspectives

Ideal Curriculum for International Cyber Incident Management Legal Studies

by Eneken Tikk, M.Jur.

Try to imagine a lawyer who would help you to resolve issues related to cyber incident management. As there is only little time to react, he or she should probably quickly understand the essence of the action and be practical about the recommended steps to take. This is a lot easier said than done, as lawyers must be thorough and base their advice on existing legal and policy frameworks.

Regarding cyber incidents, these frameworks may not always be easily identified or understood. There are different legal areas involved and often the essence of the cyber incident in question first needs to be legally qualified in order to understand in which legal domain the solutions fall. For example, an intrusion into a network may be very disturbing, but not necessarily criminal. It may also be far more serious than just a single criminal intention and fall into the legal notion of terrorist activities. Drawing a line between different concepts and deciding on the application of a specific area of law is a challenging task. A further complicating factor is the inconsistency in terminology regarding cyber incidents, which hinders development of a common policy approach to cyber security.

Not only is it likely that different legal regimes come into play in order to resolve a situation (e.g., basic information security legal requirements for business governance, criminal law or potentially law of armed conflicts), it is also the case that what may be clear in one country, may not be granted in another. While there are countries that have supported in their legislation the quality and availability of logs or the cooperation between national CERTs, etc., there are other countries that have little or no regulation on cyber security and jurisdictions. Also, since there are different national authorities and processes involved, the same legal provision may be differently implemented in different countries.

This all makes resolving an internationally relevant cyber incident quite difficult. And it is even more difficult to find a lawyer who could understand all the different legal regimes involved and practices implemented. Therefore, an ideal curriculum of cyber incident management legal issues would, first of all, give lawyers a basic understanding of the technical environment of their work — the technologies, basics of cyber security management, and relevant policies and strategies. Then, it would cover the legal aspects of daily cyber security to support lawyers' orientation in the practical aspects of preventing network intrusions or information leaks.

Naturally, the curriculum would touch upon the criminal policy and law in the field, indicating not only what has been agreed upon at the international level in terms of prohibited activities and practical criminal cooperation, but also covering individual country practices in implementing different international agreements and policy documents. It would address the unique features of cybercrime and the difficulties in solving the cases (such as no borders in cyber space, identification issues, jurisdiction problems, etc.). It would also provide the background required to debate policy issues such as "do we need a cyber terrorism treaty?" and "what do we actually mean by that?"

Also, the curriculum would indicate other perspectives of cyber incident resolution and relevant risk assessments, involving concerns of military, diplomats, intelligence, business and policy experts. Such a curriculum would also include discussion of new concepts of law,

(Continued on Page 15)

Infrastructure Protection Education and Risk Management

Panel Discussion, including:

- Barbara Yagerman, DHS Office of Infrastructure Protection, Partnership and Outreach Division.
- Ed Jopeck, Director and Immediate Past President of SARMA.
- Will McGill, Penn State University, Assistant Professor of Information Sciences and Technology.
- Maeve Dion, CIP Program Manager, Education and Cyber.

Part of the 3rd Annual Security Analysis and Risk Management Association (SARMA) Conference at the Arlington campus of George Mason University, in partnership with the Center for Infrastructure Protection (CIP) at the George Mason University School of Law.

Conference features confirmed Keynote Speakers:

- Mr. Peter F. Verga, Deputy Under Secretary of Defense for Policy Integration and Chief of Staff to the Under Secretary of Defense for Policy

- Ms. Tina Gabbrielli, Director of the Office of Risk Management and Analysis, U.S. Department of Homeland Security

- Mr. Roger W. Cressey, President of the Good Harbor Consulting Group and former Director for Transnational Threats on the National Security Council.

16 - 18 June 2009

Agenda and registration information available on the event website.

EMPP-CIP *(Cont. from 2)*

Saturdays, in addition to two multiple-day residencies.

As a public policy program, EMPP-CIP combines perspectives on business and government, law and economics, culture and technology while emphasizing critical infrastructure protection and resilience. The EMPP-CIP concentrates not only on administration but also on management and judgment as these relate to policy formulation and implementation.

Executive Education

The EMPP program is the newest addition to the extensive range of program options offered by the George Mason University School of Public Policy (SPP). Currently offering five Master's degrees and a Ph.D. in Public Policy, SPP attracts nearly 1,000 students from the U.S. and abroad, and has one of the largest public policy doctoral programs in the country. In addition to degree programs, the School conducts short-term professional development programs for corporate and government executives and organizes frequent public forums.

With its 70 full-time teaching and research faculty, 30 high-level adjunct teaching faculty, and nearly 40 professional staff, SPP maintains twelve research centers, and external research support averages more than $8 million a year, making it the number one program in its field for federal and total research expenditures as ranked by the National Science Foundation. ❖

For more information on the EMPP-CIP, contact Christine Pommerening cpommere@gmu.edu.

Perspectives *(Cont. from 13)*

policy, international coordination, etc.

Finally, an ideal curriculum would look at the most severe cases where cyber incidents may involve political or coercive motivation and involve nation states as targets or initiators and discuss how much of the law of armed conflict is applicable to cyber incidents. It would look at strategic and tactical offensive and defensive aspects of information operations (IO) by state and non-state actors to achieve political, military, and economic goals through IO means.

An ideal is likely never quite real. But after some research, it seems that it is not so difficult to imagine a master's program that would offer all these perspectives. There are a number of universities in the United States, Europe and elsewhere that have established LL.M. programs to educate law students in practical aspects of cyber conflict and whose programs, although somewhat differently focused, could be integrated into a holistic approach to what a legal cyber response team needs to have as their background knowledge.

The Center for Infrastructure Protection has started working on the details of an ideal curriculum that would provide national and international lawyers from industry, government, and academia with the "big picture" of cyber conflict and therefore help them meaningfully approach the issues brought up by their employers, without losing track of where their solutions fit into in a wider perspective. We

(Continued on Page 17)

CIP *(Cont. from 12)*

protection sectors. Samples of critical infrastructure protection issues that are included in the training curriculum include: defining critical infrastructure; assessing current threats; analyzing risk and vulnerability assessment methodologies; establishing baseline security criteria; emergency planning; and examination of specific sectors such as transportation, energy, water, and agriculture.

For more information about this training program, please view the following website: http://www.arc-tc.com/pages/index.asp.

Critical Infrastructure Awareness
Advanced Distributed Learning Course
The Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

Created at the behest of the NATO Conference of Commandants of Alliance Defense Colleges, the course is a Canadian product offered for use by NATO members and Partners. This course is intended for current and prospective strategic-level decision makers (civilian and military) who wish to enhance their knowledge and awareness of critical infrastructure protection. The course emphasizes European examples of critical infrastructure protection.

"The Canadian Defence Academy provided the technical and instructional design expertise for the course development." Other members of the development team included subject matter experts from the Canadian Forces College and the Public Safety and Emergency Preparedness Canada (PSEPC), recognized experts in the critical infrastructure protection field. ❖

Course History:

"In 2002, the NATO Conference of Commandants agreed to examine the question whether or not Critical Infrastructure Protection would be a suitable subject to be taught at Defence Colleges. The Canadian Forces College (CFC) Commandant at the time, Brigadier General Gagnon, agreed to lead a coalition of the willing to examine the question. Thirteen countries partook in a working group led by CFC which identified the objectives and teaching points."

— LCdr (RET) Robert Charest, Deputy Manager of the Project

For more information about this course, please click here.

ERM *(Cont. from 3)*

associations, the American Public Power Association and the National Rural Electric Cooperative Association, in identifying and building audiences for the training. ❖

For further information about this project, contact the program director, Dr. Brien Benson, George Mason University, 703-993-3171, bbenson@gmu.edu.

Manual *(Cont. from 8)*

not receive PCII protections.

As you read this Manual, you may have questions regarding PCII Program procedures. Please do not hesitate to contact us at pcii-info@dhs.gov or (202) 360-3023. We welcome your feedback and are glad to discuss how PCII protections may be applied to information shared with the Federal government. ❖

For more information on the PCII program, please visit: http://www.dhs.gov/PCII.

Perspectives *(Cont. from 15)*

welcome involvement by any and all subject matter experts who are interested in this effort. Please contact Eneken Tikk or Maeve Dion. ❖

CAPTAP *(Cont. from 10)*

available to help with regional CIP efforts.

DHS IP is planning to make this an annual conference; check the Web page below for conference announcements. ❖

For More Information

Visit IP's CAPTAP Web page on DHS.gov for a more detailed description of the program (http://www.dhs.gov/xinfoshare/programs/gc_1195679577314.shtm).

To learn more about C/ACAMS, e-mail the C/ACAMS Project Office at ACAMS-info@hq.dhs.gov, call 703–235–3939, or visit: http://www.dhs.gov/acams.

The Center for Infrastructure Protection works in conjunction with James Madison Univerity 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 Center is funded by a grant from the National Institute of Standards and Technology (NIST).

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