The Critical Infrastructure Protection Program June 2006 / Volume 4, No. 12

THE CIP REPORT

International CIP

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

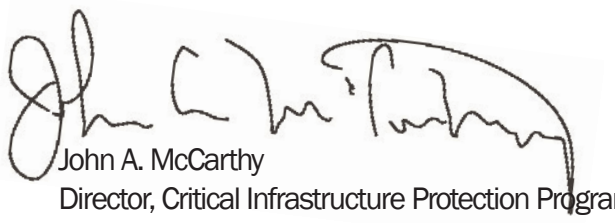
GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

This issue marks the third annual publication of *The CIP Report's* International CIP edition. In it, we not only engage our partners around the globe in a discussion of their CIP activities and accomplishments, but provide an international forum in which the same critical themes can be examined from a diversity of view points. Each echoing the importance of themes such as information sharing, public- private cooperation, and the value of strengthening international relationships, we are pleased to have contributions from Australia's Critical Infrastructure Protection Branch, Attorney General's Department, Sweden's European Crisis Management Academy and Swedish Emergency Management Agency, and Public Safety and Emergency Preparedness Canada.

Adding to the diversity of viewpoints in this issue, we have three interesting articles chronicling trips taken by a CIP Program staff member and faculty members from both George Mason University and James Madison University, our partner in the CIP Program. These articles provide an opportunity to see the unique partnerships just being built within academic institutions in China and ongoing academic inquiry that goes straight into prison camps housing terrorists.

In addition to these pieces, we also include an overview of the CI²RCO Conference on Critical Information Infrastructure Protection, which was held in Rome on March 30, 2006, and a highlight of an intern project undertaken this summer in conjunction with the Department of Homeland Security's Office of General Counsel, Infrastructure Partnerships Division.

This issue also marks the end of our fourth volume of The CIP Report, with 47 separate issues released to date. We hope that, as we enter into our fifth volume, our readers continue to provide us with the feedback, insight, and contributions that greatly enhance this monthly publication. As we seek to explore topics relevant to this CIP community, we encourage you to share with us the ideas and issues that you would like to see discussed, and we appreciate your continued readership and support.



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

Critical Infrastructure Protection in Canada

Critical infrastructure protection (CIP) continues to be one of the most important challenges facing nations today. Recent events have shown that natural disasters like floods, earthquakes, and forest fires, as well as technological failures such as blackouts, can cause tremendous damage to critical infrastructure. Canada is advancing CIP work on a number of fronts across the public and private sectors and in collaboration with the United States. This article highlights some of the recent initiatives undertaken by Public Safety and Emergency Preparedness Canada (PSEPC) in critical infrastructure protection.

National coordination

PSEPC develops initiatives and programs aimed at assuring the continuation of essential services to Canadians in the event that any part of the nation's critical infrastructure is disrupted or destroyed. It promotes a national partnership among private and public-sector stakeholders. As most of Canada's infrastructure is privately owned, the Government of Canada fosters cooperation and communication to provide the best possible assurance of a resilient and viable infrastructure. While individual sectors and provincial, territorial, and municipal governments may have their own preparedness programs, PSEPC provides national coordination to assure continuity of services across all sectors.

New legislation

Events in recent years have challenged governments and the private sector, stretching their ability to cope with emergencies. As a result, the Government of Canada announced a review of the Emergency Preparedness Act to better meet the range of events facing Canadians and to deal more specifically with new areas such as critical infrastructure protection. This process resulted in the Emergency Management Act bill being tabled in the House of Commons. The purpose of the bill is to strengthen the government's readiness to prepare for, mitigate the impact of, and respond to all hazards in Canada. It recognizes that emergency management in an evolving risk environment requires a collective and concerted approach between all jurisdictions, including the private sector and non-governmental organizations. This proposed new Act reflects a comprehensive all-hazards approach to emergency management.

National strategy

In November 2004, PSEPC published the Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection. This document helped stimulate a national discussion on the key elements required for greater protection of national critical infrastructure, and provided a basis for national consultations during the spring of 2005. These discussions with other levels of government and the owners and operators of Canada's national critical infrastructure identified measures already underway to better protect critical assets and services, and explored the gaps and challenges to protection measures.

As a result of these consultations and follow-on sessions in 2005 and 2006, PSEPC will release a National Critical Infrastructure Protection Strategy that outlines the priority areas for CIP. These include ways to share and protect information better, ways to understand interdependencies better, and roles and responsibilities for undertaking protective actions.

Education

In keeping with these priorities, several educational initiatives are underway to promote understanding of CIP issues. PSEPC's Canadian Emergency Management *(Continued, Page 16)*

TRUST
The Critical Ingredient in Australia's Critical Infrastructure Protection Strategy

Like the United States, the vast majority of Australia's critical infrastructure is owned or operated by the private sector. This means its protection can only be achieved by government and business working together.

The concept - and the benefits - of working together are easy to understand. The challenge is to take the idea of government and business sharing information, ideas, and expertise and putting it into practice. This is the real challenge of critical infrastructure protection. And it is an area where Australia has worked hard to achieve positive results and practical outcomes.

The TISN

To establish a genuine relationship with business, Prime Minister John Howard re-iterated in November 2001 the Government's determination to engage with industry and break down barriers and reservations at the very highest levels. This set the stage for an ongoing commitment from all parties to address critical infrastructure protection issues.

A key outcome was the establishment of the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) in April 2003. The TISN now works with industry across nine groups, known as Information Assurance Advisory Groups (IAAGs) - and reports to the Critical Infrastructure Advisory Council (CIAC). In turn, the CIAC reports directly to the Australian Attorney-General. This direct line to government ensures that the work done on the ground feeds directly into policy development. The TISN is very much focused on practical results - something that business finds particularly valuable.

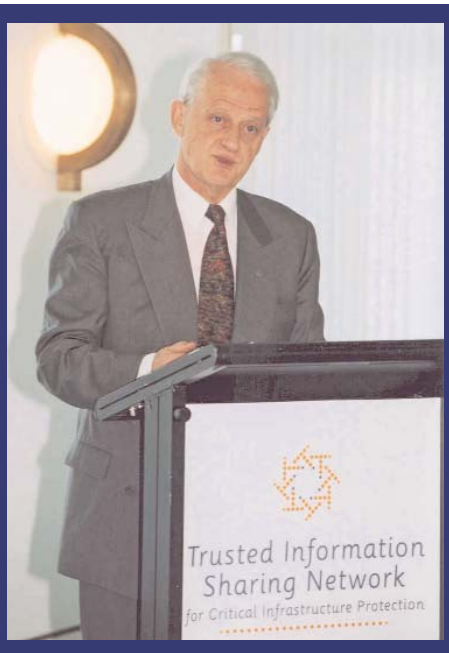
In a comparatively short time, the TISN has matured to a stage where members are looking beyond their own sectors and are now working on cross-sectoral issues.

CIPMA

One program which helps us understand the relationships that exist across individual sectors is the Critical Infrastructure Protection Modeling and Analysis (CIPMA) Program.

Through a series of linked computer models, CIPMA will map the dependencies within and between critical infrastructure sectors and facilities in Australia to better understand their relationship. From a natural disaster in a regional area, to the loss of a gas compressor station or electrical substation, CIPMA will become an invaluable aid for decision makers in critical infrastructure protection, counter-terrorism, and emergency management.

In developing CIPMA, Australian organisations involved in the program have visited key US agencies, including the Department of Homeland Security and the national laboratories at Argonne, Los Alamos, and Sandia. The support provided has helped stimulate progress in Australia to the stage where proof-of-concept demonstrations have been successfully completed. The three business sectors currently involved - banking and finance,
(Continued, Page 4)



Australian Attorney-General Philip Ruddock addresses a meeting of the Trusted Information Sharing Network

Australia's Critical Infrastructure Advisory Council reports directly to Attorney-General Philip Ruddock

Australia *(Cont. from Page 3)* communications, and energy - will be joined by a fourth sector shortly.

CNVA

TISN members are also involved in the Computer Network Vulnerability Program (CNVA). Under the Program, the Government provides co-funding on a dollar-for-dollar basis to enable businesses to engage independent IT experts to carry out thorough assessments of their computer systems and networks.

The experts look for vulnerabilities, examine the connections between computer systems and networks, and test the ability of the systems to resist exploitation and attack.

The beauty of the CNVA Program is that it provides assistance to businesses to identify vulnerabilities and other related problems before they can create a problem. Where no weaknesses are found, the reassurance this provides for the board and for stakeholders is invaluable.

SCADA

Another IT security issue the TISN is currently working on involves Systems Control and Data Acquisition (SCADA) systems. The TISN is supported by an IT Security Expert Advisory Group which has formed a community of interest for SCADA users. Following a series of workshops around Australia in 2005, the community of interest has developed a risk management framework and is establishing a portal for their users to exchange information.

Legal issues

Of course, the work of the TISN and the development of projects like CIPMA and CNVA cannot happen unless the private sector is comfortable with the way information is shared and used with other businesses and with government.

Initially, there were concerns about government freedom-of-information rules, the confidentiality of information, and the potential misuse of commercial-in-confidence information. To address these concerns, a Deed of Confidentiality has been developed to protect sensitive information and ensure information shared in the TISN is not used for commercial purposes. But it is not this formal mechanism that makes the TISN work. Members are sharing information because of the way the TISN is structured and the culture of trust that it fosters. Meetings of sector groups only involve key owners and operators of critical infrastructure and key government officials. Everyone comes together in the spirit of protecting the nation's critical infrastructure. And the result is a genuinely collegiate and cooperative atmosphere that is underpinned by mutual trust and respect. The idea of using shared information for commercial gain is no longer a significant issue for the TISN members.

Bilateral and multilateral activities

Australia realises that there is much to be learned from the experiences and expertise of other countries. Since the TISN was formed, its members have been actively involved in the regular bilateral talks program with the United States, and with delegates attending the last three rounds of talks in *(Continued, Page 15)*

Mike Rothery is the Assistant Secretary of the Critical Infrastructure Protection Branch, Attorney General's Department

Future Challenges for Crisis Management in Europe

Louise Mwinyipembe

European Crisis Management Academy

On May 3-5, 2006 the Swedish Emergency Management Agency (SEMA) and the European Crisis Management Academy (ECMA) organized a conference entitled "Future Challenges for Crisis Management in Europe" that took place in Stockholm, Sweden. Ninety participants from all over the world represented a wide range of universities, organizations, and government authorities.

Ann-Louise Eksborg, Director General of SEMA, Sir David Omand, former Security and Intelligence Co-ordinator in the Cabinet Office (UK), Ambassador Alyson J. K. Bailes, Director of the Stockholm International Peace Research Institute, and Neal A. Pollard, Outreach Chief at the US National Counterterrorism Center, all gave keynote speeches at the conference.

The aim of this multidisciplinary conference was to discuss the latest developments in crisis management, gain insight and share experiences in the field, and develop solutions to crisis management problems. A fundamental point of departure for the conference was that the separation of internal and external security is becoming less relevant. Convergence, connectivity, and complexity are key words when discussing shared threats and challenges, but also opportunities, in an increasingly interdependent world. It is critical that engaged and informed leadership is established in Europe and across the Atlantic to be able to effectively and legitimately protect and safeguard human life, maintain and develop political, economic, and social structures, and uphold common democratic values.

The conference was organized around four parallel workshops:

"Critical infrastructure protection: vulnerable systems, modern crises, and institutional design" (Moderators: Associate professor Arjen Boin, Leiden University, Dr. Allan McConnell, University of Sydney). *(Continued, Page 6)*

SEMA, the **Swedish Emergency Management Agency**, became operative on July 1, 2002. Although its acronym may suggest a mirror of the Federal Emergency Management Agency (FEMA) in the United States, SEMA has similar responsibilities to those of the US Department of Homeland Security. Responsibilities include supervising and encouraging preparedness and capacity building by all actors in society to prevent and manage a broad spectrum of strains on society in peacetime and in war.

A severe strain on society is defined as a situation that arises suddenly with little warning, which threatens fundamental societal functions and values and demands swift and coordinated consequence management. Such events can, in a worst-case scenario, lead to a breakdown of the rule of law and other institutions that uphold the principles of democracy.

The agency has a mandate to allocate government funds for various capacity building programs across society. It is responsible for scanning the national and international horizons, which together with annual vulnerability assessments from all government actors, provides a comprehensive threat assessment. Allocating research funds is an important part to ensure knowledge building to better understand present and future challenges. Moreover, the agency is responsible for coordinating IT security issues and emergency communication functioning between the local emergency services.

For more information please visit www.krisberedskapsmyndigheten.se.

SEMA/ECMA *(Cont. from Page 5)*

Modern societies are increasingly reliant upon functioning critical infrastructures, including telecommunications, IT, water systems, energy, and transport. This dependence is accompanied by increased vulnerability. As critical infrastructures become more and more complex and interlinked, it is difficult to protect them from breakdowns. A minor disruption in one system can rapidly snowball into other systems and paralyse society, which also makes critical infrastructures an attractive target for attack and exploitation. This workshop explored the causes, characteristics, and consequences of critical infrastructure vulnerability. Participants discussed strategies that can limit the vulnerability of these systems and help system managers deal with disruptions.

"European Union Crisis Management: the interface between EU member states and Union institutions" (Moderators: Dr. Magnus Ekengren, Swedish National Defence College, Dr. Mark Rhinard, Swedish Institute of International Affairs)

The role of the European Union (EU) is increasingly important in European crisis management. The Union has been involved in several crises: the Balkan conflicts, the mad cow crisis in 1996, the flooding in Central and Eastern Europe (2002) and the tsunami disaster in 2004. The expectations on future EU crisis management cabability is high, especially in the European security and defence policy areas. The challenges are great. Union institutions have traditionally fostered security among EU member states by facilitating trade and communications. The role of the Union today, however, is to create crisis management capabilities based on a proactive, strategic relationship between its institutions and the member states. To a large extent, EU crisis management involves coordinating the views and capabilities of EU member states. This workshop examined the opportunities and constraints of EU crisis management capability with a special focus on the interplay between Union institutions and member states. Participants explored new challenges from a historical-institutional perspective, and discussed the need for reforms and possible new forms of EU cooperation in the field of crisis management.

"Escalation from disaster to catastrophe: policies, plans, and uncertainty in complex, metropolitan regions" (Moderators: Professor Louise Comfort, University of Pittsburgh, Dr. Sanneke Kuipers, Leiden University)

Metropolitan regions are complex systems where dynamic interactions between physical, engineered, and socio-economic environments create conditions that are vulnerable and can escalate from routine emergencies into extreme events. These conditions include rapid population shifts from rural regions, increased burdens on civil infrastructure due to delayed maintenance, and changing economic and social bases for the region. Most disaster management plans and practices do not adequately capture the interdependencies in these three risk-generating environments. Recent disaster events such as the Sumatran *(Continued, Page 17)*

EUROPEAN CRISIS MANAGEMENT ACADEMY

ecMa

In June 2000, the **European Crisis Management Academy** (ECMA) was established as a joint initiative of the Crisis Research Center at Leiden University and the Center for Crisis Management Research and Training (Crismart) at the Swedish National Defense College in Stockholm. ECMA is a European network for approximately one hundred crisis managers and academics with an interest in research, training, and development of this field.

For more information please visit www.ecm-academy.nl/

China: Change, Uncertainty and Complexity

Dr. A. Jerry Benson, Dean - College of Integrated Science and Technology
James Madison University

During the 2006 spring semester, James Madison University (JMU) Deans Robert Reid, College of Business, and A. Jerry Benson, College of Integrated Science and Technology (academic home of the CIP Program at JMU), along with Dr. Ping Wang, Associate Professor in the College of Business's Computer Information Systems department, had the opportunity to visit China. The purpose of the trip was to discuss possible collaborative activities with targeted Chinese universities. The trip and these possible collaborative activities are building on an already existing successful JMU summer program in China. During the eleven day trip, Drs. Reid, Wang and Benson met with University administrators and faculty at Chang'An University (Xian), Sichuan University (Chengdu), Shandong University (Jinan), Northeastern University (Shenyang), Shandong University - Weihai (Weihai), and Tsinghua University (Beijing). All of the institutions are 985 project (top 34 universities in China) or 211 project (top 100 universities) designees and, thus receive national support.

China has emerged, and continues to develop momentum, as a major player in the global economy and the geopolitical landscape. This has especially been true in their goal of building a high tech economy and is reflected in the government, directly driving the focus, through funding, of graduate education, increasing the number of science-technology-engineering-mathematics (STEM) graduates, and university-related research and development. Infrastructure items of transportation, energy, and information networks are of top priority. Advances and economic competition in these areas offer opportunities for conflict or creative, collaborative solutions. For example, it was recently reported that the motor vehicle population in China increases about 23 percent per year. Currently only around 2 percent of the population operate motor vehicles, so the potential for growth is significant. At this pace, the number of motor vehicles will double in four years. Concurrently, estimates show that approximately one half of the world's easily accessible oil has been drilled. Either we can continue to compete for the same limited resources or we can begin to develop collaborative research, technology transfer and business practices that benefit both nations.

The change China is undergoing also reflects uncertainty and complexity. The focus on science, technology, and business opens the door for potential collaboration without directly raising issues of human welfare and social justice. Yet, with their growing emphasis on higher education and international collaboration, will these areas not soon be forced to change also? The complex, and still existing, relationship *(Continued, Page 8)*

Drs. Benson, Reid, and Wang visit Chang An University in Xian.

China *(Cont. from Page 7)*
between the People's Party and academic direction and administration reflects a system undergoing a tenuous transition of power and leadership. Also, there is a growing gap between the small minority leading and participating in the high-tech emphasis and growth and the large majority of citizens still living in the rural, agricultural, and sometimes third world conditions. The goal to transition an economy built on the advantage of cheap labor to one that is competitive in quality, as well as cost, reflects further societal uncertainty and complexity. The budding recognition that growth bears environmental, as well as human, impact must be addressed. During the visit, (granted the interactions were almost solely with university affiliated individuals), the visitors perceived a growing recognition that for China to be a true world player, the complexities of growth and change must be addressed with an interrelated systems perspective.

The very systems that promote collaborative potential also present in some ways the greatest risk. A good example of this is the area of information technology. The visitors had the opportunity to observe very strong programs in software development and productive technology transfer of university research and development into the commercial world. They also experienced tremendous interest in JMU programs in information security and infrastructure assurance. As institutions of higher education in the United States, we have the opportunity to share our knowledge and practices, thus building more secure information technology systems that will support further international collaboration. Yet, from a governmental perspective, this raises issues of perhaps diminishing our own national government or private sector security. At the national level, building a trustful partnership will take time and will only grow from productive relationships at the individual to individual and like entity to like entity level.

As has been reported elsewhere, the Chinese university system is transitioning from the Russian system of specialized institutions to the western comprehensive university model. Along with this is a great interest among Chinese faculty to learn and implement some of the variety of western instructional pedagogies. Even with the expansion of higher education and a move toward comprehensive universities, it was still clear that the direction of research funding, which then dictated curricula emphasis, was set by the government. At Chang'An University, there was a focus on transportation - intelligent highway systems, materials science related to road construction issues, and operations management and technology regarding supply chains. At Sichuan University the emphasis was on air transportation. Northeastern University has highly developed programs in software development and expressed an interest in advancing their accounting program to world-class standards. And, at Tsinghua University, approximately 50 percent of their funding comes from government and industry contracts or grants.

Discussions were held about possible student exchanges (a 2+1+1 undergraduate program is favored in China with the Chinese student spending the junior year in a US institution focused on specialized studies in their discipline), faculty exchanges, program and curriculum development, collaborative undergraduate and graduate dual degree programs, and collaborative research projects. James Madison University has extended invitations for three faculty from the universities visited to spend a portion of the 2006-07 academic year at JMU. James Madison University's current program, under Dr. Wang's leadership, involves students from across all JMU colleges who spend 6 to 12 weeks engaged in a curriculum focused on themes of world history, the history and culture of China, comparative politics, study of the Chinese language, international business - business environment and operations in China, and Taiji Quan. The program is based at Tsinghua University in Beijing. From the institutions visited, the University will continue dialogue with selected institutions to explore further collaborative program development. ❖

Legal Insights

International Student Visas and the Student Exchange and Visitor Information System

Colleen Hardy, CIP Program

Colleen Hardy

With the five year anniversary of the deadly September 11th terrorist attacks rapidly approaching, the United States is still coping and learning from the tragedy. An important lesson learned from the attacks was the lackadaisical process surrounding international student visas. Two of the hijackers from the 9/11 attacks were in the US on student visas - neither one had ever set foot in a US school. Two other 9/11 hijackers applied for student visas and received them - six months after the attacks. Additionally, at least one of the terrorists responsible for the 1993 bombing of the World Trade Center entered the country on a student visa. Clearly, there was a major glitch in the process and immediate attention was both essential and necessary.

Before the terrorist attacks in September 2001, the Immigration and Naturalization Service (INS) was working on ways to improve the international student visa process and accounting system. One such system was the Student Exchange and Visitor Information System (SEVIS). However, after the 9/11 attacks, they increased their efforts to implement SEVIS as soon as possible.

On May 10, 2002, Attorney General John Ashcroft announced that SEVIS would be in operation by July 2002 and would be mandatory for all schools to implement by the following January. Ashcroft stated, "the United States of America will not allow our welcome to be abused by those who disguise themselves and their intentions." SEVIS is an automated system for tracking student visas and establishes several requirements on schools hosting international students. The INS and US consulates will be connected via the Internet with thousands of higher learning institutions who enroll international students. The schools must enter information about each student into the INS's system.

Before applicants can be granted a visa, they must attend a one-on-one interview with a State Department consular in the applicant's home country. However, they must be accepted to a school before they can schedule the interview. Additionally, applicants must pay a $100 non-refundable fee for the SEVIS application process.

It is the responsibility of the school to keep the system updated. For example, the school must report within 24 hours if an international student drops out, fails to show up, or is disciplined for criminal behavior. Additionally, the school must report if the student changes their name or address at the beginning of a new term or if they do not take a full course load of classes. When SEVIS was first initiated, it decreased the amount of time students were allowed to spend in the US before classes commenced. Before 2002, students were allowed to arrive 180 days before school started; SEVIS changed that to 30 days. The State Department recently raised the number of days to 45.

An international student visa allows a student to enter the US legally. According to the USA Study Guide's website, to be applicable for such a visa, the applicant must be in good health (applicants who have tested positive for HIV will not be allowed to enter the *(Continued, Page 10)*

First CI²RCO Conference on Critical Information Infrastructure Protection

March 30, 2006
Rome, Italy

CIP Program Director John McCarthy was featured at this Critical Information Infrastructure Protection (CIIP) conference, which was hosted by the Critical Information Infrastructure Research Co-ordination Project (CI²RCO), a Co-ordination Action co-funded under the Information Society Technologies Priority of the 6th Framework Programme by the European Commission.

CI²RCO focuses on research and development related to the protection of information and communication technology infrastructures, within and across public and private sectors. CI²RCO began in March of 2005 as a two-year project, and the leadership quickly organized a European CIIP network that included public and private research organizations, agencies, academia, policy makers, and CII stakeholders.

The goals of CI²RCO include:
(1) promoting a coordinated, Europe-wide strategy for CIIP R&D (including the member states and the candidate countries); and,
(2) establishing a European Research Area on CIIP.

After holding several workshops throughout 2005, CI²RCO hosted its first international conference on March 30, 2006, in Rome. The aim of the conference was to further expand and integrate the network of CIIP researchers. The conference attendees shared information on existing CIIP R&D initiatives, opportunities for collaboration, and current and future CIIP R&D requirements. The report of the conference (including all speakers' materials) is available at http://www.ci2rco.org/ under "Events." CI²RCO's *European CIIP Newsletter* is also available from their website.

The conference included several European speakers, and CI²RCO invited John McCarthy and Derek Bopping (Defence Science and Technology Organisation, Australia) to present additional international perspectives. McCarthy briefly overviewed the history of CIIP in the US and discussed the Federal government's role in CIIP R&D. He also spoke about the current CIIP environment, including the various threats to CII and the challenges (technical, organizational, legal, and behavioral) to providing protection. The slides and white paper from John McCarthy's presentation are available at http://cipp.gmu. edu/research /CI2RCO-2006.php ❖

Legal Insights *(Cont. from Page 9)*
US on a international student visa), the applicant must agree to obey all US laws, they must be able to support themselves financially while studying in the US, and finally, the applicant must agree to leave the US when their course of study is complete.

By August 2003, 5,937 schools had complied with the SEVIS requirements and over one million students were registered to attend school in the US. After SEVIS' first year of implementation, the Immigration and Customs Enforcement (ICE) announced that 8,737 schools and exchange visitor programs had complied with SEVIS. By July 2004, 9,500 campuses were SEVIS certified and more than 770,000 visa-holding students' and exchange visitors visas had been accepted to study in the US under SEVIS. ICE also reported that 36,000 potential student violators were reported for not showing up for classes, expulsion, suspension, or failure to maintain a full course load. These violations led to the investigation of over 1,500 cases and 155 arrests.

The number of international students studying in the US noticeably declined after the 9/11 attacks. However, the Council of Graduate Schools' (CGS) admission survey for Fall 2006 stated that there was an 11% increase in international graduate applications compared to fall 2005. The CGS's report also stated *(Continued, Page 15)*

A democracy confronts terrorists.

Michael I. Krauss
Professor of Law
George Mason University

The following is an excerpt written by Professor Michael Krauss, an Academic Fellow of the Foundation for the Defense of Democracies and Professor of Law at the George Mason University School of Law. Prof. Krauss took part in a mission to Israel in 2005 to explore responses to terrorism in a democratic society. The article is written as a "journal entry" and explores aspects of the mission.

Gilboa Prison, June 1, 2005.

It was the third day of our trip. We were exhausted but thrilled. Eighteen (in my case - up to thirty for a few others) hours of flying had landed us in Israel, on our mission [funded by the DC-based Foundation for the Defense of Democracies (FDD)] to investigate the nature of and the responses to terrorism in the country surely most afflicted by it. I had been scrunched in the middle of the middle section of a jumbo-jet, next to a kindly little old lady whom I was unwilling to wake up on the overnight flight, full bladder notwithstanding. Then I was exposed, with my 36 academic colleagues, to two full days of lectures immediately after our arrival, jet lag equally notwithstanding. No free time yet, no time to even really venture outside our Tel Aviv hotel.

Now, however, we were on the road. We were over one hour from Tel Aviv - in miniscule Israel that means we were almost as far away as one could get - at a location intriguingly missing from the country's very detailed road maps. We were at Gilboa junction, near Afula, a forbidding-looking maximum-security prison solely for terrorists. Having heard from professors defining and describing terrorists for two days now, we were about to hear from the terrorists themselves.

We were briefed by the prison Commander, a Colonel and a Druze (the first of several non-Jewish Israelis we would encounter in positions of high military authority) who explained to us the make-up and structure of Gilboa Prison. Gilboa (where Saul and Jonathan died fighting the Philistines) houses 850 of Israel's 5500 terrorist convicts. [Israel also has about 20,000 other criminal convicts in "normal" prisons.] The Gilboa inmates are divided into six mini-prisons, each housing about 100 men - one mini-prison for Israeli citizens and five housing non-Israelis: that is, in practice, citizens of the Palestinian Authority. The Israelis must serve out their term: there is no parole for terrorist murderers (but there is no death penalty for them, either). The non-Israelis are occasionally released because of political agreement, regardless of the heinousness of their acts, and so they are housed separately from Israelis so as not to destroy their morale. Every single inhabitant of all six mini-prisons was a Muslim-- Jewish terrorists, only a handful in number, are housed in solitary confinement in a different prison to protect them from other inmates. We also learned that there were no Christian Arab terrorists at Gilboa, and in fact, the Christian population of Judea and Samaria (the West Bank portion of the Palestinian Authority) had declined tremendously because they had been made unwelcome by Hamas, Islamic Jihad, and Hezbollah.

[Aside: a few in our (largely Christian) group wanted to know about Jewish and Christian terrorism, as if such phenomena must exist in the same way as Muslim terrorism. There are Jewish and Christian terrorists in the world, but you don't read about them strapping on explosives and heading for the local bus station. Importantly for FDD, the likes of Timothy McVeigh, Eric Rudolph and the barest handful that constitute the fringes of the Kach group are so miniscule in number that they simply don't threaten our democratic way of life as Islamo-fascist *(Continued, Page 12)*

Israel *(Cont. from Page 11)* terrorists do. Anyone looking for "balance" by suggesting that Christian and Jewish terrorists are just as much a problem as the Jihadis is unnecessarily paralyzed by political correctness.]

We were led into the courtyard of one of the mini-prisons, the one housing the Israeli (Arab) citizens. Half the inmates were in the courtyard, where they may spend half of each day eating, smoking, talking, or playing basketball if they wish. We inspected a cell, and were shocked to find a true mini-kitchen consisting of a hot plate, metal utensils (including small knives), and a television set (tuned to Al-Jazeera). Home-cooked meals with groceries provided by the inmates' families, it turns out, are permissible if the inmate does not desire mess hall cooking.

We returned to the courtyard. The inmates had chosen one of their number, Rofi, a slender thirty-something man who spoke pretty good English, to be their spokesman. They surrounded us, fifty maximum security inmates literally pressing against thirty-odd American academics (including several young women) and three unarmed guards. The warden was not in sight, and the guards kept beyond earshot, so as to avoid the appearance of intimidation of the inmates. It was a surreal experience. We asked the spokesman where he learned his English; he responded that he had taken many English courses at the Hebrew University in Jerusalem. We asked him about his sneakers, emblazoned as they were with a red maple leaf and the word "CANADA" in boldface. He informed us that many members of his extended family lived in Canada. Political refugees under that country's liberal admission policies, perhaps? Does someone in Ottawa at least know about Rofi?

We asked him why he was in prison. He told us it was a travesty of justice. He had never been convicted, but was awaiting trial. Of what had he been accused, we asked (we were troubled by this, as the Druze prison commander had assured us that this mini-prison housed only convicts, not suspects). He replied that he was charged with "helping someone perform an operation." Asked what he meant by "an operation", he responded evasively, saying that sometimes someone from another village asks to know where a particular building is located in Jerusalem, and so maybe he tells that friend, but he is not responsible for what that friend does with the information, which was public after all. He closed with an entreaty that we tell the world, tell American media, about the "conditions" at Gilboa. One of our number, a criminologist, responded that the conditions in fact looked pretty good to her. Rofi reacted by repeating that he was incarcerated without trial. He added that old men were here, and pointed to a man who appeared about 60 years old. We asked Rofi what that man had done to merit confinement at his age. Rofi fell silent.

We later asked the prison commander to corroborate his earlier statement that the mini-prison we visited was for violent convicts; after all, Rofi was merely accused of providing information, and had not even been tried. The commander (who, like many Israelis we met during our stay, spoke no English - we used an FDD member to translate from the Hebrew) smiled and disappeared into his office for a minute. He emerged with Rofi's "sheet." Rofi, it turned out, was neither an accused nor a mere "helper." Rofi was a Hamas member in the tenth year of a 20-year term imposed for sneaking up behind a young Israeli waiting at a bus stop, and slitting his throat. Why, we wondered to the commander, would Rofi tell us such a blatant lie? Because, we were told with a wry smile to our interpreter, most media folks who interview Gilboa prisoners don't bother to double-check their stories.

Two other inmates asked Rofi to translate what turned out to be the only honest "grievance" we heard at Gilboa prison. They were angry that they were with the Israeli citizens, because they resided in the Golan Heights (which Israel annexed after the 1967 war, bestowing instant Israeli citizenship on all inhabitants). The men considered themselves Syrian (Syria had used the sparsely-populated Golan to lob bombs onto Israeli kibbutzim located in the flatlands below - whence Israel's refusal to relinquish this land). They conceded that *(Continued, Page 17)*

INTERN UPDATE

National Security and International Law: Information Flow in Foreign Waters

Jordan Davies, CIP Program Legal Intern

A delicate balance must be achieved between informing the private sector of important national security matters and ensuring that the information is not used by foreign entities to cause destruction to our critical infrastructure.[1] Concerns may arise when the US government gives sensitive information to the private sector -- e.g., via security alerts from the Department of Homeland Security (DHS) or through law enforcement and counter-terrorism methods -- because of the potential for subsequent access by foreign entities.

In order to understand how this critical information may be accessed by foreign entities and to ensure critical infrastructure information is monitored effectively, much attention should be focused on the relevant laws of these countries. Foreign regulatory, licensing, and security laws should be examined to discover the means by which the information may be disseminated beyond the individual business. We must begin to learn how foreign governments, both ally and enemy, can obtain information from their constituents, and how third parties can then obtain the information from foreign governments.

For example, in the Commonwealth of Virginia, there are approximately 250 Canadian-owned companies.[2] The Canadian government could potentially gain access to any sensitive information that DHS provides to these companies. One possible method is through the Canadian Security Intelligence Service Act (CSISA), which closely resembles the USA PATRIOT Act. CSISA provides for disclosure of information to the government if, upon reasonable grounds, Canada's "national security interests" are at risk.

Since Canada has always been considered a close ally, this information transfer may not at first seem much of a threat. However, once this information is in the hands of the government, the flow of information can be reversed through Canada's "freedom of information" laws. Much like FOIA, Canada's Access to Information Act provides any citizen access to unclassified information and essentially, the "right to know."

Many countries today have laws that resemble FOIA. Japan has a "Law Concerning Access to Information Held by Administrative Organs." Likewise, in Turkey there is a "Turkish Law on the Right to Information." Since each nation's laws are different, there could be a wide spectrum of accessibility under FOIA-like foreign laws. It is possible that information which the US FOIA would prevent from being disclosed could become accessible through another country's laws.

It is imperative for our government to predict where sensitive information will end up once it is provided to the private sector. What is the solution? There are endless possibilities once information is poured into the stream of commerce. It is fundamental that the government contemplate and then try to resolve the issues associated with such information sharing before a problem arises. ❖

Jordan Davies is a Canadian citizen currently working towards his J.D. He recently finished his first year at Liberty University School of Law in Lynchburg, Virginia. This summer internship with the CIP Program has him working with Mr. Carlos Kizzee, Esq. of the Department of Homeland Security's Office of General Counsel, Infrastructure Partnerships Division. Prior to law school, Jordan worked at a sport law firm in Atlanta, Georgia. After law school, his goal is to enter the J.A.G. corps.

[1] Although this article addresses only foreign-owned businesses located in the US, a comparable analysis should be made as to US businesses operating abroad.

[2] Roxana Tiron, *Canadian Embassy Ramps up Lobbying,* THE HILL NEWS, Mar. 1, 2006, http://www.hillnews.com/thehill/export/TheHill/Business/030106_canada.html

A Traveler's Observations in the Middle East

Meghann Rother, CIP Program

Meghann Rother is an Assistant Program Coordinator for the CIP Program's Private Sector Program. She is currently pursuing a Master of Arts in Government at The Johns Hopkins University, where her research focuses on identity and terrorism.

Despite being regularly featured in the media, the Middle East is a region about which Westerners know relatively little. Amidst the headlines describing conflict, politics, and terrorism, little is said about daily life and the people who live there. Thus, it was with great curiosity that I set out on a month-long trek through Egypt, Jordan, Syria, and Turkey on the famous Cairo to Istanbul route.

Although many people would opt for a vacation at the beach, I was eager to mingle with locals and enthusiastic about exploring new territory. While taxis in the Middle East provide an easy and inexpensive mode of transport, I opted for public transportation in an effort to delve into local life. As it turned out, local life, and transport, was much more challenging than anticipated.

The author leaving Petra via public transportation.

Nothing I encountered in the Middle East resembled what the West considers "public transportation." Instead, the network is made up of small passenger vans, or mini-buses, which operate on a basis similar to sharing a taxi. Neither the routes nor pick-up and drop-off points are marked and one must enter and exit the vehicle while it continues to move.

If this weren't puzzling enough, there is also an unspoken seating etiquette. Women traveling alone generally sit at the front; men will stand rather than sit next to an unrelated woman. This etiquette extends to other modes of transport, such as the subway, where the first two cars of each train are reserved for women exclusively. Although this practice is not posted anywhere, the female riders enforce the rule with gusto which I witnessed when an unsuspecting Japanese backpacker entered the ladies' carriage, from which he was promptly expelled with a few sharp words.

Throughout Egypt, security of critical infrastructure, and security in general, seemed to be of little concern. One exception, however, was my visit to the Sinai Peninsula where I joined a small group as there is no public transportation and foreigners are generally not permitted to drive themselves due to the area's sensitive history and strategic position. Our group was accompanied by an armed guard, a result of the extremist activities that had occurred only weeks before. The accommodation consisted of a small group of bungalows, whose main entrance was also manned by an armed guard in addition to a metal detector. Thankfully, the most taxing activity either guard had to negotiate while traveling with us was lighting a cigarette on a windy day.

Meghann Rother enjoying sunrise on Mount Sinai.

After departing the Sinai Peninsula, I crossed by ferry to Jordan and traveled overland to Syria and Turkey by train, horse, jeep, and bus. While traveling back to the United States I contemplated what type of security I would encounter upon my return given the stamps which now fill my passport. In the end, nothing more than a quick comparison between my passport and customs declaration was required. I quickly passed through immigration and, much like entry to Cairo, was unceremoniously released onto an unsuspecting population. ❖

Australia *(Cont. from Page 4)*
2003, 2004 and 2006.

One very positive outcome of this has been the establishment of dialogue between corresponding sector groups. For example, members of the Water Services IAAG attended the Technical Security Working Group and Homeland Security Science and Technology bilateral meetings held in the United States from 30 May to 2 June, and Mr. John Whitler from the Environmental Protection Agency will be the facilitator at the Water Contamination Response and Recovery Workshop in Australia from 25 - 27 June.

Australian government agencies also participated in this year's Cyberstorm exercise which was coordinated by the US Department of Homeland Security. Cyberstorm tested procedures, communication channels, and response capabilities in the event of a cyber attack and international communication protocols between countries.

Within the wider Asia/Pacific region, Australia and the United States are both involved with the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC-TEL), and the Computer Emergency Response Team (CERT) community. Australia has been heavily involved in the APEC-TEL's program to develop CERT capabilities among the region's developing economies.

Conclusion

Australia's approach to critical infrastructure protection recognises that it is best achieved when all parties work together and share information in an open and trusted environment. Since its inception, the TISN has evolved to become a trusted information sharing network, both in name, and in practice.

The fact that this exchange of information and experiences now extends between Australia and the United States reflects the close ties that exist between both countries. By continuing to work together, we can develop better and more innovative ways to protect our critical infrastructure. By doing so, we also reinforce the common economic, social, and democratic foundations that bind our two countries together. ❖

Legal Insights *(Cont. from Page 10)* that there was an increase of applications from China and India. David Wilson, the Associate Dean and Director of CGS, stated that the increase in applications could be credited to many things, including increased recruitment, word of mouth, and the Federal government's focus on reducing visa processing delays and denials. The report indicates that international student applications are on the rise again; however, they are not quite as high as they were before 9/11.

The United States is actively recruiting international students. However, now we are competing for international students with countries such as Australia, England, and Canada. Those countries have greatly increased their recruitment and efforts to obtain more international students. For example, the United Kingdom established a new immigration policy to attract more international students.

International students are both vital and essential to the US. According to NAFSA: Association of International Educators, in 2004, foreign students generated $13.3 billion for the national economy. More importantly, international students can foster relationships between their home country and the US. Therefore, it is imperative for the government to maintain SEVIS so that it continues to encourage international students to study in the United States but also protects the US from those who may abuse our welcome. ❖

Canada *(Cont. from Page 2)*
College (CEMC) will be offering a CIP awareness course to Federal government managers responsible for emergency management and/or for the oversight of critical infrastructure sectors. This course is designed to better prepare Federal employees to conduct business continuity planning and to support the implementation of Canada's National Critical Infrastructure Assurance Program (NCIAP). In addition, CEMC has collaborated with the Canadian Defence Academy and the Canadian Forces College in the development of CIP course material that can be broadly shared within Canada and throughout the North Atlantic Treaty Organization (NATO) sphere of influence. The aim of this collaborative educational initiative is to create a general awareness of CIP for middle to senior level NATO leaders, both civilian and military.

In addition, PSEPC and the Natural Sciences and Engineering Research Council of Canada have collaborated to fund academic research projects that will study the interdependencies of Canada's major infrastructure systems. Known as the Joint Infrastructure Interdependencies Research Program (JIIRP), it is the first research program of its kind in Canada. JIIRP is designed to help infrastructure owners and operators better understand the extent of their dependencies on other sectors for delivering their services and goods, and how the risks resulting from these interdependencies can be mitigated.

Cooperative action

Horizontal programs such as JIIRP and government-private sector partnerships are developed through the framework of the NCIAP. The short-term goal of this program is to bring together organizations with a stake in better assuring critical infrastructure so that the exact nature of the partnership and methods of information exchange can be designed. In 2005, for example, the Private Sector Working Group on Pandemic Influenza Planning was established with Canada's ten critical infrastructure sectors. This group provided information on both avian and pandemic influenza and sectoral views on a whole-of-government approach to addressing these threats. Through similar consultation and planning, PSEPC will continue to advance cooperative actions and partnerships between governments and the private sector.

Cross-border infrastructure

Critical infrastructure protection is a shared responsibility in the North American context, with Canadian and US critical infrastructure becoming increasingly interconnected. About 50 percent of Canada's oil production and nearly 60 percent of Canada's natural gas goes to the US market through pipelines that cross the border. Canada is now the largest source of imported crude oil for the United States, so a sustained disruption to a major oil pipeline would have significant consequences for the U.S. economy.

The Security and Prosperity Partnership (SPP) of North America has been instrumental in focusing joint CIP strategies between Canada and the United States. This partnership is crucial not only for governments, but also for the private sector, as the protection of integrated North American infrastructures is vital to the daily operation of communities and national economies. The SPP commits the two governments to conducting joint vulnerability assessments of critical border infrastructure, including energy, dams, telecommunications, transportation, nuclear and radiological, defense, industrial, and cyber systems. The SPP also commits both parties to working together to enhance the protection of cross-border infrastructure.

A basis for progress

Canada has made much progress in critical infrastructure protection, but a great deal of work remains to be done. The programs, policies, and initiatives outlined above provide a basis for strengthening Canada's ability to assure the continuation of essential services. This will be an ongoing task requiring continued focus and effort. ❖

SEMA/ECMA *(Cont. from Page 6)* earthquake and tsunami in 2004 and the hurricanes on the US Gulf Coast in 2005 demonstrate how natural hazards can rapidly trigger massively destructive consequences for both regions and populations. In this workshop, participants explored the interaction between physical, engineered, and socio-economic conditions that create disaster risks in metropolitan regions. They also considered strategies that may reduce these risks in a synergistic effort to achieve sustainable disaster management.

"Cooperating against terrorism: EU/US relations post September 11" (Moderators: Dr. Magnus Ranstorp, Swedish National Defence College, Director Lars Nicander, Swedish National Defence College).

This workshop sought to identify and assess the current state of the US-EU trans-Atlantic partnership within the framework of counter-terrorism policies at the global level (GWOT), and regionally through bilateral dialogue, focusing specifically on intelligence architecture and the issue of countering radicalization and recruitment of the next generation of salafist-jihadi extremists. Participants synthesized the latest academic and senior policy-making perspectives, and discussed common and divergent views of future strategies in an asymmetric global threat environment. ❖

Israel *(Cont. from Page 12)* they had killed an Israeli because he was a Jew, but they wanted to be in the "foreign" mini-prison with the PA citizens, where they could be released as the result of a political deal (one massive deal, releasing 400 murderers and their accomplices in return for three kidnapped Israeli soldiers, was announced during our stay). ❖

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 (ZRA) 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://cipp.gmu.edu/report/.