

THE CIP REPORT

International Updates

CIP: An International Look . . . 2

Canada's Progress Report . . . 4

UK Civil Contingencies Act . . . 6

Legal Updates 8

Critical Conversation Report . . . 9

U.S. State Dept Initiatives . . . 10

CRIS: International Institute . . 11

Political Economy of Terrorism
Conference 12

Newsletter Editorial Staff

John McCarthy, *Director /
Principal Investigator*

Jessica M. Milloy, *Special
Assistant to the Director / CIP
Report Co-Editor*

Amy Cobb, *Senior Project
Associate*

Jeanne Geers, *CIP Report Co-
Editor*

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

Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to
The CIP Report please click
[here](#).

Visit us online for this and other
issues at <http://cipp.gmu.edu>

In May of 2004 we released a special international edition of *The CIP Report*, providing an overview of critical infrastructure protection efforts from around the globe. In the year since this issue was released, significant legislation has been passed and progress has been made in many of the countries we originally highlighted and in a few nations not originally included, warranting another issue focusing on these changes.

While domestic critical infrastructure protection issues continue to challenge industry, government, and academia on a daily basis, we cannot overlook the importance of international issues in critical infrastructure protection. Beyond the physical networks such as pipelines and cargo security, our infrastructures are as vulnerable to domestic cyber attacks as they are to attacks originating overseas, especially with the global reach of industry. Our industries know no national bounds; likewise, best practices in CIP should include those that have been developed by our international colleagues. As each nation works to address these critical issues, we must ensure that we work in concert and collaboratively to best harness the valuable resources at our disposal in facing this international need.

In this issue of *The CIP Report*, we have highlighted legislative and organizational changes in critical infrastructure protection around the globe, as well as initiatives such as the State Department's International CIP Policy Outreach Team, the International Institute for Critical Infrastructures, and a progress report for Canada. While by no means comprehensive of all CIP activities and accomplishments around the world, these articles provide insight into some of the significant changes that have taken place over the course of the past year.

Additionally, we have also included reviews of two recent events, the Critical Conversation on cybersecurity held at the National Press Club, and the Political Economy of Terrorism Conference held at the George Mason School of Law. Finally, we would like to invite you to visit our new webpage (<http://cipp.gmu.edu/>). The site includes more information on our Program and will serve as a collection of critical infrastructure protection resources, which we will add to over the weeks and months to come.



School of Law
CRITICAL INFRASTRUCTURE
PROTECTION PROGRAM

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

CIP: An International Look

**Tim Goobic, CIP Program Intern
University of Kentucky**

Critical infrastructure protection takes on a number of different shapes depending upon the environment in which it is set. In the United States, CIP efforts are largely coordinated and initiated by the Department of Homeland Security, but other nations have chosen to secure themselves in different ways, some more similar to the US federal approach than others.



Australia may be considered the most similar

nation in that the Attorney General's department has taken the lead in creating CIP policy. One of the most crucial components created has been the Trusted Information Sharing Network (TISN), which is comprised of public and private critical infrastructure owners and operators who alert each other when potential security issues arise. This TISN is ultimately supervised by the Critical Infrastructure Advisory Council. Over the past year, the government has expanded in numerous ways through such actions as the Computer Network Vulnerability Assessment Program and the Research Network for a Secure Australia, which funds experts to identify and protect vulnerable public assets and aims to increase

overall CIP research respectively.



The Canadian approach is also similar,

as it has created the National Critical Infrastructure Assurance Program (NCIAP) to build a working partnership between the public and private sectors. As in the US, over 80% of Canadian critical infrastructures are run by private industry or non-government organizations. The NCIAP is situated under the Public Safety and Emergency Preparedness Canada (PSEPC) department, with the overall responsibility of protection from natural disasters and terrorist activities. A discussion paper about the NCIAP was first distributed in November of 2002 for discussion amongst various stakeholders. Since then, progress has been made for better information sharing and overall cooperation between public, private, and international parties, but there is still significant work to be done. *(For more information, see article on Page 4.)*



The United Kingdom was slightly slower in the creation of a comprehensive system of security. After

years of deliberation, the Civil Contingencies Act was passed in 2004 by Parliament and subsequently received Royal Assent. Instead of centralizing power and authority, the legislation focused more on equipping and preparing local responders. Local responders are either categorized as those who will have duties placed upon them, such as emergency services, or those who are responsible for co-operating and sharing information, such as utility and transportation networks. The Act improves local planning and information sharing, and ensures that local activities are in line with regional and national authorities.



Sweden has created the central authority Swedish

Emergency Management Agency (SEMA). This agency has a clearly defined hierarchical structure, situating councils and delegations associated with SEMA, an executive board, and an executive director at the top. After deciding on strategy and a course of action, orders are passed down the ranks to the administrative and information departments. From there, commands are given to the research, planning, emergency *(Continued, Page 3)*

International CIP (Cont. from Page 2) management, RAKEL (public safety radio), technical, and information assurance and analysis departments. Established in 2002, SEMA was the result of years of discussion about how the nation should best protect and respond to serious infrastructure disruption, terrorist attacks, dangerous epidemics, or full-scale war. However, while this may look like centralized power, SEMA actually does more to strengthen emergency preparedness from the bottom up, by preparing local municipalities and county boards to handle a crisis. Local authorities are expected to adequately secure six broadly defined areas of security in their specific region. Ultimately, all levels of government are working together, resulting in a stronger degree of coordination. Integration of SEMA has gone well, though there are some tasks, such as the legal formulization of new roles that municipalities have (and compensation related to it), which have not yet been finalized.



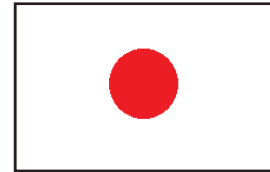
Efforts to improve the protection of Switzerland's critical infrastructure have been underway since the 1997 Strategic Leadership Exercise, further emphasized by the 2000

Security Policy Report, which made it a key issue when it stated that national security pertained to people, resources, and critical infrastructure. Rather than consolidating power at either the national or local levels, Switzerland decided to strengthen, expand, and refine departments and agencies that were already in place. Of the 11 agencies listed in an update from the Centre for International Security Policy, the first two listed, the Swiss Federal Strategic Unit for Information Technology and The Swiss Coordination Unit for Cybercrime Control, deal with protection from cyber attacks.



This past April, the European Union drafted material which seeks to establish a crisis management arrangement for the EU. It would be created for mutual protection against attacks on infrastructures which are shared resources among those nations. The report calls for Parliament to create an organic structure by the end of 2005. The EU has lofty ambitions in this matter, calling upon member states to share relevant information, as well as respect the privacy rights of citizens. Finances

will be provided by the general EU fund and a workable relationship is hoped to be established between public and private sectors in order for mutual security to be attained.



The Japanese are the most dissimilar from

the United States in terms of critical infrastructure protection, as responsibilities are divided up between a number of separate agencies. Some have suggested that in order to better protect itself, a new strategy should be taken. Lincoln Bloomfield Jr., Assistant Secretary of State for Political-Military Affairs, made a statement at the US-Japan CIP Forum in late 2004, that "the designation of a central coordinating entity for the nation...is essential to be able to command the attention of the disparate sectors of the economy and independent government departments and coordinate a national cyber security effort."

Though nations are dealing with CIP in their own ways, it is obvious that the past four years have seen more attention and resources focusing on this area. Critical infrastructure protection has emerged as a global issue in which nations will continue to learn from one another. ❖

Securing an Open Society: Canada's Progress Report

On May 11th of this year, Canada's Deputy Prime Minister, the Honourable Anne McLellan tabled in Parliament *Securing an Open Society: One Year Later*, a progress report on the implementation of the nation's *Securing an Open Society: Canada's National Security Policy*. When the Report was tabled, the Deputy Prime Minister stated:

*"The Government is committed to enhancing national security and has made significant progress implementing initiatives identified in the National Security Policy as well as additional national security measures. Although efforts to improve Canada's national security system must continue, important steps have been taken and the progress report provides an important measure of our success."*ⁱⁱ

This progress includes addressing significant gaps in Canada's security system, in further



Former Secretary Tom Ridge and Canadian Deputy Prime Minister Anne McClellan sign a joint border initiative in late 2004.

strengthening Canada's threat assessment, prevention and response capabilities, and implementing a number of initiatives identified in the policy. Notable examples include the establishment of the Integrated Threat Assessment Centre (ITAC). ITAC's primary objective is to produce comprehensive threat assessments, which are distributed within the intelligence community and to relevant first-line responders, such as law enforcement, on a timely basis. Its assessments, based on intelligence and trends analysis, evaluate both the probability and potential consequence of threats. Such assessments allow the Government of Canada to more effectively coordinate activities in response to specific threats in order to prevent or mitigate risks to public safety. Canadian security will increasingly depend on the country's ability to contribute to international security.

Accordingly, the Government of Canada, through ITAC, is promoting a more integrated international intelligence community by developing liaison arrangements with foreign intelligence organizations, including the Joint Terrorism Analysis Centre, in Britain, the National Counterterrorism Center in the United States; and the National Threat Assessment Centre in Australia.ⁱⁱ

A new Government Operations Centre has been established to

provide stable, around-the-clock coordination and support across government and to key national players in the event of a national emergency.ⁱⁱⁱ Canada's capacity to prepare for and respond to health emergencies has also been strengthened with the creation of the new Public Health Agency of Canada (PHAC) and the appointment of Canada's first Chief Public Health Officer. The creation of PHAC marks the beginning of a new approach to federal leadership and collaboration with provinces and territories on efforts to renew the public health system in Canada and support a sustainable health care system. Focused on more effective efforts to prevent chronic diseases, like cancer and heart disease, prevent injuries and respond to public health emergencies and infectious disease outbreaks, the Public Health Agency of Canada works closely with provinces and territories to keep Canadians healthy.^{iv}

On April 19, 2005, the Government issued *Canada's International Policy Statement-A Role of Pride and Influence in the World*, the country's first integrated plan designed to strengthen Canada's role in the world. The Statement assesses the need for Canada to invest in its defence and security, international commitments and foreign aid in order to support a strong international role. It outlines a targeted approach, (*Continued, Page 5*)



Dr. David Butler-Jones is Canada's first Chief Public Health Officer.

Canada (Cont. from Page 4) based on Canadian strengths and values that will enable Canada to focus its efforts in order to be more effective and influential.^v

A key element of the National Security Policy is the establishment of the Cross-Cultural Roundtable on Security, created to engage in a long-term dialogue on matters related to national security as they impact a diverse and pluralistic society. The Government needs the help and support of Canadians to make its approach to security effective. The Roundtable will provide a forum to discuss emerging trends and developments emanating from national security matters and it will serve to better inform policy makers. The Roundtable held its inaugural meeting on March 7, 2005.^{vi}

Canadian relations within North America are of the utmost importance in ensuring a stronger, more secure and more prosperous Canada. The North American countries have made major advances since 9/11 in developing improved security policies, systems and processes. With our improved and expanding rela-

tions at all levels, we now have opportunities to further our common security goals in an evolving and strengthened North American relationship. At their meeting on March 23, 2005, Prime Minister Martin, U.S. President Bush and Mexican President Fox launched the Security and Prosperity Partnership of North America.^{vii} The Security aspect of this partnership commits the countries to establishing a common approach to security to protect North America from external threats, to prevent and respond to threats within North America, and to further streamline the secure and efficient movement of legitimate, low-risk traffic across shared borders. In the 90 days following this meeting, experts from the United States, Mexico and Canada have proposed specific strategies and objectives to meet these goals. These North American strategies and objectives, once fully implemented by the bilateral and trilateral working groups now engaged, will lead to the development of new avenues of cooperation that will make North American open societies safer and more secure, businesses more competitive and economies more resilient.

The NSP stated that the Government of Canada would release a position paper establishing the key elements of a proposed National Critical Infrastructure Protection Strategy. The key elements create a (Continued, Page 15)

Canadian National Critical Infrastructure Town Hall Presentation

Toronto, Canada – May 19, 2005. The department of Public Safety and Emergency Preparedness Canada (PSEPC) hosted a town hall on the nation's Critical Infrastructure Protection Strategy to generate support for the Canadian National CIP Strategy from the invited provincial, municipal, sectoral and private owner representatives. Speaking on the topic of U.S. and International CIP and Cyber Security Coordination was John McCarthy, Director of the George Mason University Critical Infrastructure Protection (CIP) Program, the only invited speaker from the United States.

In addition to John McCarthy, speakers from Canada focused on the importance of critical service availability to international infrastructure systems and dialogue centered on how each government is currently addressing critical infrastructure protection (CIP) and cyber security. Under McCarthy's leadership since 2002, the CIP Program focuses on key areas of critical infrastructure research, addressing topics such as cyber security, physical security, and information sharing between public and private sectors. During his presentation, McCarthy noted that all of the key elements addressed within the Canadian position paper are shared by the United States.

The protection of the critical infrastructure is unique because these critical services know no national bounds, particularly in the area of cyber security. As each nation works to address critical infrastructure issues, events such as this will further encourage international groups to work collaboratively to best harness the valuable resources needed in facing this international problem.

The United Kingdom's Civil Contingency Act

Chris Burrow
University of Virginia

The UK's Civil Contingencies Bill became an Act of Parliament on November 18, 2004. The Act is intended to "deliver a single framework for civil protection in the UK." Like the Homeland Security Act of 2002 adopted in the US, the UK law modernizes civil preparedness responsibilities and organizations. Unlike the approach taken in the US, however, the UK government is not creating a new department or consolidated agency to address evolving security challenges.

The UK bill focuses principally on resilience at the local level. National resilience, the UK government concludes, will follow from local preparedness and response capabilities. Like Congress and the Bush Administration, UK government officials are struggling to balance local, regional, and national solutions. In defining roles and responsibilities, the UK bill delegates significant authority to local administrators, rather than regional or national responders and government entities.

The Civil Contingencies Draft Regulations and Guidance for Emergency Preparedness identify the major responsibilities of emergency preparedness as cooperation, information sharing, risk assessment, business continuity management, and communicating with the public. The burden of emergency pre-

paredness falls mostly on Category 1 responders, or public sector authorities. They must fulfill duties in all of these categories of activity, relying on the assistance of the Regulations, the Guidance, and Category 2 responders.



Category 2 responders, which include most infrastructure owners in the UK, also have significant responsibilities. They must share information regarding their civil protection work and cooperate with Category 1 responders in the risk assess-

ment process. In other areas of preparedness, such as emergency planning, business continuity management, and communicating with the public, Category 2 responders are governed by their own regulations, but still have a duty to assist Category 1 responders in carrying out their responsibilities with regards to these functions. The table below distinguishes between Category 1 and Category 2 responders.

Responsibilities:

Cooperation. The principle mechanism for multi-agency cooperation in the Act is the Local Resilience Forum (LRF). The Draft Guidelines for the Act specify that the main LRF (*Continued, Page 7*)

Category 1 Responders	Category 2 Responders
County, Metropolitan, and Borough Councils	Electricity Suppliers
Unitary and State District Councils	Gas Suppliers
Police Forces	Water Undertakers
Fire Authorities	Telecommunications Operators
Ambulance Authorities	Railway Operators
Trusts	Airports
Environment Agency	Ports and Harbors
Maritime and Coastguard Agency	Health and Safety Executive

Civil Contingencies Act (*Cont. from Page 6*) must meet at least twice a year and a regular cycle of meetings should be developed. The forums are expected to produce:

- risk profiles;
- a coordinated approach to emergency planning, business continuity management, and public warning; and,
- coordination of multi-agency agreements, protocols, and exercises.

The Act broadens the range of Category 2 organizations that will engage in the civil protection process, though their involvement in the process is more limited than that of Category 1 responders. The Draft Regulations state that Category 1 responders must keep Category 2 responders informed of when and where the meetings will take place, as well as the planned agenda. The presence and involvement of Category 2 organizations in LRFs are to be dictated on a "right to attend, right to invite" basis. These organizations may send representatives to any meetings of an LRF they deem necessary, but are discouraged from attending if they cannot add value to a discussion.

Information Sharing. The Act specifies that responders have a duty to share information that involves civil protection. Category 2 responders have already agreed to put as much civil protection information into the public domain as possible, though there are several categories of

information that cannot be released to the public. This information may be formally requested by a Category 1 responder so that proper precautions can be taken to protect the information.


The Draft

Regulations identify four different types of sensitive information:

- information prejudicial to national security;
- information prejudicial to public safety;
- commercially sensitive information; and,
- personal information.

Both categories of responders are expected to make reasonable requests. Category 1 responders may appeal to higher authorities if reasonable requests for information are denied, while the Draft Guidance for Preparing for Emergencies notes that sanctions are set out in the Act to protect Category 2 responders from any mishandling of information that may occur.

Risk Assessment. The Act places a duty to perform risk assessments on Category 1 responders. The Draft Guidance for Preparing for Emergencies provides a six-step process that Category 1 responders must follow in performing their risk assessment:



Bruce Mann is the Head of the Civil Contingencies Secretariat (CCS). The CCS was set up in July 2001 to improve the UK's resilience against disruptive challenges through working with others to anticipate, assess, prevent, prepare, respond and recover. The CCS defines resilience as the ability at every level - national, regional and local - to detect, prevent and if necessary handle disruptive challenges. A key focus of the organization is to support the Civil Contingencies Act.

1. Contextualization
2. Hazard and threat identification and allocation
3. Assessing the likelihood of hazards
4. Assessing the impact of hazards
5. Risk treatment
6. Monitoring and reviewing

Category 2 responders are expected to cooperate with Category 1 responders in the risk assessment process. The Draft Regulations stipulate that as a part of the local resilience forum, Category 1 responders must coordinate with themselves to maintain a community risk register to collect the risk assessments that each responder has performed. This risk register must be shared with the members of that local resilience forum and the responders of neighboring forums that may be affected by the assessments.

Emergency Planning. The majority of the burden of risk planning will also fall on Category 1 responders. These responders will be expected to carry out their *(Continued, Page 14)*

International Legal Updates

Maeve Dion, CIP Program, Legal Researcher

The following updates represent international legal and legislative developments in security and critical infrastructure protection over the past year.

Australia

- Individuals charged with, or convicted of, certain terrorism offenses now face a presumption against bail (bail would only be granted in "exceptional circumstances").
- Similar to the already-required aviation industry employee security checks, the government introduced maritime security identification cards, requiring a security assessment requisite to employment in the maritime industry.
- The government tightened restrictions in criminal trials, further protecting the disclosure of sensitive information that could threaten national security.

Canada

- In April of 2005, Canada approved the creation of the Canada Border Services Agency and the Department of Public Safety and Emergency Preparedness, which integrates the activities of the previous Department of the Solicitor General, the Office of Critical Infrastructure Protection and Emergency Preparedness and the National Crime Prevention Center.

European Union

- In February of 2005, the EU Council adopted a Framework Decision on attacks against information systems, detailing the actions that each member state should criminalize, including:
 - unlawful, intentional access to an information system;
 - "intentional serious hindering or interruption" of an information system; and
 - intentional interference (deletion, alteration, etc.) with data on an information system.The decision also directs each member state to define its jurisdiction to include (1) offenses committed by individuals located within the member state's territory (even if the information system is located elsewhere), and (2) offenses committed against information systems located within the member state's territory (even if the perpetrator is located elsewhere). The Framework Decision can be found [here](#).
- In April of 2005, the EU Commission instituted legal proceedings against ten member states for infringement of EU rules for electronic communications. Although many of these rules addressed commercial and consumer issues, one of the member states, Poland, was cited for not instituting emergency services access via the single European emergency number. More information can be found [here](#).

Japan

- In April of 2005, Japan increased personal data protection with its Personal Information Protection Law. Businesses that store personal information on 5,000 or more individuals must comply with this law. According to an IDG News Service interview with a Japanese lawyer, the law defines personal data to include "a person's name, address, date of birth, sex, home and/or mobile phone numbers and also a person's e-mail address if that (*Continued, Page 13*)

Are We Serious About Cybersecurity?

A Report from the May 18, 2005 Critical Conversation

Amy Cobb, Senior Project Associate, CIP Program

In recent weeks and months, news organizations have reported security breaches to multiple networks in the government and private sector, affecting millions of people. On May 18, 2005, the Critical Infrastructure Protection Program hosted *Getting Serious About Cybersecurity*, the fourth in a series of Critical Conversations on the nation's post-9/11 preparedness and how to better protect America's critical infrastructures. Frank Sesno, Senior Fellow of the CIP Program and GMU Professor of Public Policy and Communication, moderated the event. His first question to panelists, "What are the most urgent priorities if we're to get serious about cyber security?" was extremely timely. On this same day, the Cybersecurity Enhancement Act of 2005 bill was on the House floor. The bill contains far-reaching implications including the elevation of the cyber security position within the Department of Homeland Security to Assistant Secretary.

The panelists, agreeing that the administration needs to take cyber security more seriously, did not debate the actual elevation of the position, but rather where this authority would reside. Representative Zoe Lofgren (D-CA) asserted that she voted against the original bill that formed DHS knowing the new department would spend the first three years simply getting organ-

ized. However, Lofgren feels "we have the department now, even though I questioned the wisdom at the outset, and I think it's important

"I think it's important that [the cyber security chief] be given the authority to get the job done. And especially in the area of cyberspace -- where, you can't see it, touch it, feel it, taste it - - it tends to be ignored."

Representative Zoe Lofgren

that they be given the authority to get the job done. And especially in the area of cyberspace – where, you can't see it, touch it, feel it, taste it – it tends to be ignored."

Representative Tom Davis (R-VA) agrees the position should be elevated, but should not reside in DHS, "an agency that got an F on its own FISMA last year." He feels the White House, and more specifically OMB, would be the right place for the job because "they have the juice when it comes to procurements to make sure that everything interconnects, that

the safety is broad."

Lofgren had allies on the panel including Paul Kurtz, Executive Director of the Cyber Security Industry Alliance. Kurtz said that the private sector is "missing that chief, we're missing that quarterback that is out there to chart the course... And it would be nice to have that chief back or someone at the Department of Homeland Security who can, if you will, offer that strategic thinking, that beacon that the private sector can work with."

Marian Hopkins, Director of Public Policy at the Business Roundtable, supports leadership in critical areas; however, the nation's leadership want to handle it, so long as it gets done. "Frankly, in terms of an Assistant Secretary ... my take on it is do both (DHS & OMB) – do whatever it takes in order to elevate cyber security within the federal government. The (Continued, Page 13)



Paul Kurtz, Frank Sesno, Rep. Tom Davis and Marian Hopkins discuss the Cybersecurity Enhancement Act of 2005.

US Department of State: Taking the Lead on International CIP Outreach

International Critical Infrastructure Protection Policy Outreach Team

The goal of US international Critical Infrastructure Protection (CIP) policy is to shape the international environment to reduce the risk to critical US and foreign national information and physical infrastructures on which the US and its allies depend for their national security and economic well-being.

The US Department of State CIP policy and outreach program is based in the Office of Plans, Policy, and Analysis in the Bureau of Political-Military Affairs. For cyber infrastructures, the program proceeds from the conviction that the US cannot guarantee the reliability, availability and integrity of its information infrastructure if the foreign infrastructures to which it is inextricably linked are not secure. For physical infrastructures, this program is predicated on the fact that the US depends heavily on specific allied and other physical infrastructures for force projection, forward military deployments and flows of goods.

This program was implemented in 1998 under authorities that include PDD-63, E.O. 13231 (revised by E.O. 13286, March 1, 2003), the 2003 *National Strategy to Secure Cyberspace* and the associated *National*

Strategy for the Physical Protection of Critical Infrastructure and Key Assets, and HSPD-7 *Directive on Critical Infrastructure Identification, Prioritization, and Protection* (December 17, 2003).

The *National Strategy for the Physical Protection of Critical Infrastructure* calls on the Department of State to support the development and implementation of sector protection initiatives by laying the groundwork for bilateral and multilateral infrastructure protective agreements with our international allies. The more recently published HSPD-7 repeats this call, recognizing the Department of State's role of working with foreign countries and international organizations to strengthen the protection of United States critical infrastructure and key resources. Additionally, the *National Strategy to Secure Cyberspace* directs the Department of State to lead federal efforts to enhance international cyberspace security cooperation.

International CIP Interagency Working Group

The Department has chaired an International CIP Working Group since 1999 that consists of departments and agencies with international CIP goals, objectives, and/or equities. Outreach initiatives are developed and con-

ducted as an interagency process. The Department synthesizes interagency-specified goals and develops a foreign policy strategy designed to achieve them. The interagency process requires constant coordination, review, and revision. One does not craft an international strategy once and allow it to remain static. It changes over time based on the global environment, progress made, and changing priorities, among other factors.

The Department chairs the working group in conjunction with the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, which works in partnership with federal, state, local, private, and international entities to protect the country's critical infrastructures. Additionally, DHS's Science and Technology Directorate seeks to develop capabilities to detect and deter attacks on our information systems and critical infrastructures.

International Engagement

US interaction with other nations on issues of critical infrastructure protection consists of three avenues of engagement: bilateral; multilateral and regional; and international fora. Bilateral engagement occurs between the United States and select countries on a case-by-case basis, *(Continued, Page 11)*



State Dept. (Cont. from Page 10) whereas multilateral cooperation – the United States' preferred method of engagement – allows for interaction with many nations simultaneously. Some ongoing multilateral initiatives and regional fora in which the US is actively pursuing issues of critical infrastructure include:

- Asia Pacific Economic Cooperation Telecommunication Forum;
- Organization for Economic Cooperation and Development;
- Organization of American States;
- Southeast Europe Cybersecurity Initiative; and
- G-8 High Tech Crime Group.

Since 2000, the U.S. has also

sought to raise international awareness on cybersecurity in the UN General Assembly by promoting a series of resolutions that reflect

the US orientation to the issue. These resolutions, all adopted unanimously, have proven invaluable for subsequent outreach efforts since individual governments had already pledged their policy support. Resolutions to date include:

- UNGA 55/63, "Combating the Criminal Misuse of Information Technology," presenting awareness-raising cybercrime principles developed by the G-8, adopted December 4, 2000;
- UNGA 56/121, "Combating the Criminal Misuse of Information Technology," a follow-on resolution pointing to the Council of Europe Cybercrime Convention as a model for national cybercrime legislation, adopted

December 19, 2001;

- UNGA 57/239, "Creation of a Global Culture of Cybersecurity," a resolution bringing awareness of the OECD network security guidelines to the UNGA membership, adopted December 20, 2002; and
- UNGA 58/199, "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures," based on the G-8 High-tech Crime principles, adopted December 23, 2003.

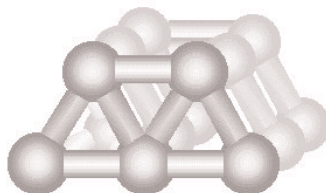
The first phase of the UN-sponsored "World Summit on the Information Society," (WSIS) took place in Geneva, Switzerland, in December 2003. Language that reflects the U.S. position was included in the resulting Declaration of Principles and Action Plan. The Department will remain an active participant in the run up to the second phase, scheduled to take place in Tunisia, November 16-18, 2005. ❖

CRIS: The International Institute for Critical Infrastructures

Electric power networks have long been recognized as being critical infrastructures of industrialized nations. In modern times, two other networks have also become critical in this sense: communication networks and computer networks.

Communication systems and computers have become indispensable in everyday life - from commercial enterprises to enter-

tainment industries - and it is difficult to imagine a life without the amenities these two systems



offer. Traditionally, electric power networks have used the computer and communication networks in a variety of critical applica-

tions. However, there are exciting possibilities to invent new configurations and organizations of power, communication and computer networks in such a way that they would be more robust in the face of catastrophes, could be controlled and protected for optimum security, economy, and performance.

The International Institute for Critical (Continued, Page 14)

Conference on the Political Economy of Terrorism

In order to better understand the current threats to national security, it is necessary to thoroughly define the enemy. Over a two day period, the Program in Economics, Politics, and Law and the CIP Program hosted a conference aimed at diagnosing the Political Economy of Terrorism. Attendees from private, public, and international arenas engaged in a structured conversation around 13 papers, each addressing a variety of topics, including religion, culture, and the economic consequences of terrorism.

The conference was facilitated by Charles K. Rowley, GMU Professor of Economics. Rowley, who is also the General Director of The Locke Institute and Director of the Program in Economics and the Law at the James M. Buchanan Center for Political Economy, spoke on his joint working paper, *The Significance of Israel and Palestine*. Largely a historical look at conflict in the region, his contention that the Israeli group Haganah was a terrorist organization inspired debate among participants as to what the standards are for defining a group as a defender of citizen rights or as a terrorist organization.

Economics professor Bryan Caplan presented a paper titled *The Relevance of the Rational Choice Model* and theorized that

terrorists can be categorized as either sympathizer, active, or suicidal. He argued that since suicide bombers only account for 1.6% of incidents, it is possible to deter, persuade, or appease the majority of terrorists. After his presentation, conference members rebutted by noting many suicide bombers act because they have contracted a fatal illness and therefore believe such a deed would allow them to become a martyr for Islam. This challenged Caplan's theory that the only irrational terrorists are the suicide bombers.

Economics Professor Eli Berman of the University of California, San Diego, sparked discussion throughout the entire event and defended his claim that terrorists are not created because of religion, but because of the community in which they develop. Berman noted that by forcing a fiscal separation of Religion and State, there will be fewer incentives for a religious sect to organize politically. With reference to Hamas, he showed how easy it is for a particular religious sect with political power to change from a humane and peaceful approach, to one which endorses suicide as a means to commit murder.

Along the same topic, Ronald Wintrobe of the University of Western Ontario presented his findings that an individual who joins a radical group will ultimate-

ly lose the desire for independent thought. His thesis that an individual's utility depends on autonomy and solidarity demonstrates that a person's beliefs are often exchanged for a euphoric feeling of solidarity. Therefore, when an individual's beliefs are that of a group, any action, including suicide, may be taken if it ultimately improves social welfare.

Three speakers presented analysis regarding terrorism and subsequent domestic economic impact. Nichols State University Professor Morris Coats lectured how current DHS spending may not be done in the most efficient manner, while Mogens Justesen from the University of Southern Denmark asserted that there was a lack of correlation between poor countries and terrorism. Justesen went on to note that democracies will not necessarily flourish following initial free and fair elections, but provided elections continue over time, insurgencies and public unrest will transform from physical violence to political debate.

The conference concluded with remarks from Rowley, noting that a majority of attendees remained throughout the entire conference because, he believes, there was an excess of quality conversation and discussion on all presented papers. Those papers will be available on the CIPP website in the coming months. ❖

International Legal Updates (Cont. from Page 8) address is recognizably the person's name." Businesses must have a corporate privacy officer, must "specify for what purpose information is being collected, obtain consent from individuals before using the information for any other purpose than the one originally stated, and take measures to prevent data being leaked and stolen." Non-compliant businesses, including managers and employees who handle the personal information, may face fines or up to six months imprisonment. The Japanese government also provided business guidelines and best practices on how to secure personal data.

United Kingdom

- In December of 2004, the House of Lords Judicial Committee found that some government powers in the Anti-Terrorism, Crime and Security Act of 2001 discriminated against foreign nationals and were not proportionate to the terrorism threats facing the UK. In response, the Home Office introduced the Prevention of Terrorism Bill into the House of Commons in February of 2005. This bill would allow the Home Secretary to issue "Control Orders" aimed at restricting the conduct of individuals suspected of terrorist activity. According to the Home Office website, the control orders "will enable the authorities to impose conditions ranging from prohibitions on access to specific items or services, and restrictions on association with named individuals, to the imposition of restrictions [sic] on movement or curfews. The controls ... would not include detention in prison although it is intended that a breach of a control order should be a criminal [sic] offence and prosecuted in the usual way." More information on the proposed legislation can be found [here](#). ❖

Critical Conversation (Cont. from Page 9) consequences are too dire if we don't."

The panel was engrossed in discussing what government was doing and not doing, what it was capable of accomplishing, and the importance of elevating cyber security within the government. However, Jody Westby, Managing Director at Pricewaterhouse-

Coopers LLP, feels corporate America has a larger role in cyber security that they have yet to take. Ms. Westby has endured nine years of frustration attempting to alert CEO's and other company executives to the critical role of IT security. Ms. Westby supports an SEC annual filing requirement that "simply requires companies to state what they are doing to protect their corporate assets".

the SEC should require an annual filing of what corporations are doing to protect assets, the industry representatives and the House representatives from both sides of the aisle see the current administration and private sector actions on cyber security issues lacking and deficient. Davis said "A cyber Pearl Harbor - unfortunately, it could very well happen and we're all kind of frustrated at the pace at which the government has been reacting to this."

The government needs more aggressive leadership in the cyber arena and must focus more funding on this area of research. The private sector needs to individually identify their security problems, assist the government and the IT industry in developing safer systems and both must work together in raising public awareness on the risks. ❖

Lofgren and others on the panel expressed concern with Ms. Westby's plan, wondering if the filings might in effect provide potential wrongdoers with an accurate map to a company's vulnerabilities.

Although the panelists agreed to disagree on whether DHS or OMB should have the elevated cyber position or whether



John McCarthy, Jody Westby, and Paul Kurtz field questions from the audience.

Civil Contingencies Act (Cont. from Page 7) functions as necessary in preventing and mitigating emergencies. They are responsible for:

- maintaining plans for preventing emergency;
- maintaining plans for reducing, controlling, or mitigating its effects; and,
- maintaining plans for taking other action in connection with the emergency.

Category 2 responders are governed by their own legislation and regulations regarding emergency planning. However, they are expected to assist Category 1 responders in emergency plan preparation and maintenance.

Business Continuity

Management. The Act requires Category 1 responders to maintain plans to ensure that they can continue to perform their functions in emergency situations as far as is practicable. The Draft Guidance for Emergency Preparedness sets guiding principles for establishing which functions must be maintained. It also specifies that responders that rely on other organizations that provide services, such as infor-

mation technology or telecommunications providers, must ensure that those service organizations can function as well in the event of an emergency.

The Draft Guidance for Emergency Preparedness establishes a methodology for business continuity management:

- Risk assessment
- Exercising business continuity plans
- Training key staff
- Reviewing and maintaining business continuity plans
- Publication of business continuity plans

Communicating with the Public.

The Act identifies two separate duties for responders in regards to communicating with the public. Responders must make the public aware of the risks of emergencies, how the responders are prepared to deal with emergencies, and what they should do when emergencies occur. The second duty is to warn the public and provide information and advice as necessary. Category 1 responders must publish all or part of risk assessments and emergency plans they have made that are

necessary or desirable to publish.

The Draft Regulations and Guidance specify that the responders should choose one organization to take lead responsibility in warning and informing the public in order to avoid duplication of effort. It should coordinate with other Category 1 responders in fulfilling its role. The Guidance recognizes that many Category 2 responders already have a duty to warn, inform, and advise their customers in emergencies as part of their own regulatory frameworks. Category 1 responders should recognize and avoid duplicating these efforts. The Guidance provides examples of good practice to aid responders in forming communications plans, as well as the training and exercises required by the Regulations.

Compliance:

The Minister for the Cabinet Office, in its Draft Regulations for the Civil Contingencies Act, includes a provision that the requirements set forth in the Regulations will not go into effect until May 15, 2006. At that date, all entities that have responsibilities as enumerated by the Regulations must be in compliance. ❖

CRIS (Cont. from Page 11)

Infrastructures, based in Sweden but with members from around the world, brings together experts to join forces for developing systems for the future in an integrated fashion, combining the capabilities, opportunities, and goals for research in the disciplines above into a unified vision. The expertise in these

fields exists in many international institutions, and the Institute intends to develop a strategy which will tap into this pool of expertise across national boundaries. The International CRIS Institute - drawing experts from different universities around the globe, and relying on international industries for support and guidance - is an ideal

framework for such an enterprise.

The objectives of CRIS are to promote, encourage and develop awareness and knowledge to increase the dependability of the critical infrastructures in society, mainly the power system, communication system and the computer network. ❖

Canada (Cont. from Page 5) basis from which the critical infrastructure protection challenge is to be met by the federal, provincial and territorial governments, as well as the industry sectors. This commitment was met when PSEPC issued the *Government of Canada Position Paper on a National Critical Infrastructure Protection Strategy* in November 2004, based on the work begun under the National Critical Infrastructure Assurance Program (NCIAP).^{viii}

The Position Paper was developed as a result of dialogue with stakeholders on concepts and issues surrounding the development of the NCIAP. The provinces, territories and industry associations shared their views on shaping the program and presented information about their existing critical infrastructure protection programs and plans. Canada's Strategy for National Critical Infrastructure Protection will be developed in a similar manner, through targeted consultations with private industry leaders representing the ten sectors (Energy, Communications and Information Technology, Finance, Health Care, Food, Water, Transportation, Safety, Government and Manufacturing) as well as various federal, provincial and municipal governments responsible for critical infrastruc-

ture protection.

Once the consultation process is brought to a close, PSEPC will be reviewing the feedback they received from their partners across the country and compiling important points on how to face the challenges of protecting Canada's national critical infrastructure. The feedback will be incorporated into an integrated and forward-looking National Critical Infrastructure Protection Strategy, completed by the end of the summer in 2005.

The above outlines examples of the progress made during the year following the release of the NSP. The Deputy Prime Minister pointed out that the National Security Policy put Canada on a long-term path to enhancing the security of this country. While progress has been made in implementing the policy, much remains to be done. Working with partners at home and abroad, the Government of Canada will continue to take steps to build a more integrated security system to better protect Canada and Canadians and to contribute to a safer world. It is the intention of Canada's leadership to fulfill this core responsibility of government in a way that ensures that Canada remains an open and welcoming society, where cultural

and religious differences are respected and fundamental human rights and freedoms are enjoyed by all citizens.^{ix}

ⁱ Full details on progress of these and other initiatives are set out in *Securing an Open Society: One Year Later*. Electronic copies of the report can be found at <http://www.pco-bcp.gc.ca/default.asp?Language=E&Page=ministers&Sub=deputygm>

ⁱⁱ Further information on ITAC can be found at http://www.csis-scrs.gc.ca/eng/backgrnd/back13_e.html

ⁱⁱⁱ Further information on the Government Operations Centre can be found at http://www.ocipep.gc.ca/info_pro/fact_sheets/general/em_gov_em_op_e.asp

^{iv} For further information on PHAC refer to http://www.phac-aspc.gc.ca/about_apropos/index.html

^v For further information on Canada's International Policy Statement refer to <http://www.dfait-maeci.gc.ca/cip-pic/ips/ips-en.asp>

^{vi} For further information on the Roundtable refer to <http://www.sgc.gc.ca/roundtable/>

^{vii} For further information SPP refer to http://www.pco-bcp.gc.ca/default.asp?Language=E&Page=Ministers&doc=deputygm/secure_message_e.htm

^{viii} For further information on the NCIAP see http://www.ocipep.gc.ca/critical/nciap/positionpap_e.asp#_Toc84996305

^{ix} For further details on the Deputy Prime Minister's statement see http://www.pco-bcp.gc.ca/default.asp?Language=E&Page=Ministers&doc=deputygm/secure_message_e.htm ❖

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

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://techcenter.gmu.edu/programs/cipp/cip_report.html.