The Critical Infrastructure Protection Program April 2006 / Volume 4, No. 10

THE CIP REPORT

Publishing

Zeichner Risk Analytics

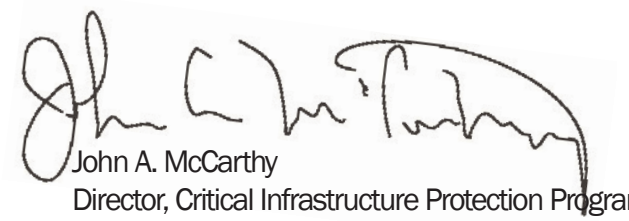
Contact: cipp01@gmu.edu
703.993.4840
If you would like to subscribe to *The CIP Report* please click here.
Visit us online for this and other issues at http://cipp.gmu.edu

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

In this month's edition of *The CIP Report*, we are pleased to feature an update on our Private Sector Program (PSP), which is focused on private industry's role in protecting critical infrastructure. The Private Sector Program component of the CIP Program began in December of 2003 and has since advanced the process of engaging the private sector as a partner in our nation's security. We first introduced this group in last April's issue, but in the year since, we have seen growth in Program activities and a change in leadership. Our Private Sector Program now supports six Sector Coordinating Councils and the Partnership for Critical Infrastructure Security. Under the leadership of Kathryn Condello, PSP continues to grow and expand the support offered to each of these groups. A description of the sectors that PSP supports, and the work of those sectors regarding critical infrastructure protection, is outlined in this issue.

In addition to an overview of the various sectors, we also have included information on the Department of Homeland Security's (DHS) Office of Infrastructure Protection's new security awareness campaign, information on the two-year anniversary of the Protected Critical Infrastructure Information (PCII) Program, and a new DHS pilot program with the Technology Management Program at George Mason University seeking to better prepare current and future generations of executives for critical security and emergency preparedness challenges.

In addition to these articles, we also include invitation materials to two new events being hosted by the CIP Program in the coming months. Building upon the success of our recently released Monograph on the Committee on Foreign Investment (available on our website at http://cipp.gmu.edu/research/CFIUS.php), we are pleased to continue this highly relevant dialogue with a panel discussion featuring Dr. Edward Graham, David Marchick, Esq., the Hon. Patrick Mulloy, and Kristen Verderame, Esq. The panel, to be held on April 28, 2006, will be moderated by Prof. William Lash, III, and a keynote speech will be provided by Stewart Baker, Esq. Additional information on each participant, as well as registration information, can be found in this issue. Finally, we are also pleased to host the 25th Anniversary Event for the Paperwork Reduction Act on June 16, 2006.



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

Private Sector Program Overview and Cross-Sector Organization

The April 2005 issue of *The CIP Report* outlined the support of the Private Sector Program (PSP), a component of the CIP Program, to public-private partnerships and their homeland security and critical infrastructure protection activities. PSP focuses its activities on private industry's role in protecting critical infrastructure while utilizing the vast knowledge developed by the CIP Program to assist in its efforts. One year later, this support of private sector activities has not only continued, but the level of activity within these private sector groups has increased. In addition, the public-private partnership model has been formalized by the recent creation of the Critical Infrastructure Partnership Advisory Council (CIPAC). Over the past two years, a number of critical infrastructure and key resource (CI/KR) sectors have formed Sector Coordinating Councils (SCCs) to discuss common security concerns and activities and also to hear from the federal government on its critical infrastructure protection programs. Initially, many sectors spent time organizing and reaching out within their sectors to form SCCs which are broad and representative. The SCCs are now maturing and are very active in developing sector specific plans and discussing policy and strategy.

Public-Private Partnerships

Owners and operators of the Nation's infrastructure, organized into 17 CI/KR sectors, along with the Federal departments and agencies charged with leading infrastructure protection activities in these sectors, have been contemplating security issues for many years.

Events in recent history, such as the Y2K transition, the September 11th terrorist attacks, and the hurricanes of fall 2005, have resulted in increased interaction between the government and the private sector. Continual concerns regarding future attacks and weaknesses in the nation's security demanded that the Federal government take necessary steps to strengthen the homeland. With roughly 85% of the Nation's critical infrastructure owned and operated by the private sector, the Federal government developed the National Infrastructure Protection Plan (NIPP), engaging the private sector as a partner in its efforts to protect the homeland.

Recognizing the need to draw upon expertise found in the private sector, and the difficulty of integrating multiple governmental agencies and the private sector, the Department of Homeland Security (DHS) proposed a sector partnership model that includes broad-based industry representative groups, termed Sector Coordinating Councils (SCCs), and corresponding GCCs. In this model, each of the 17 CI/KR sectors would have a SCC and GCC paired to work collaboratively on homeland security issues. Moreover, SCCs enable owners and operators of these infrastructures to share valuable information concerning critical infrastructure protection and discuss associated best practices. These councils also facilitate information sharing among sector partners to assist in the development of sector-related plans and policies. The private sector encouraged the creation of GCCs to decrease the amount of duplicative efforts and initiatives that were coming from government departments and agencies with similar or related missions and *(Continued, Page 3)*

The 17 CI/KR Sectors

- Banking and Finance
- Chemical
- Commercial Facilities
- Commercial Nuclear Reactors, Materials, and Waste
- Dams
- Defense Industrial Base
- Drinking Water and Wastewater Treatment Systems
- Emergency Services
- Energy
- Food and Agriculture
- Government Facilities
- Information Technology
- National Monuments and Icons
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation Systems

PSP Overview *(Cont. from Page 2)* areas of authority. The Interim NIPP, released in February 2005, initially outlined how the partnership model could be constructed.

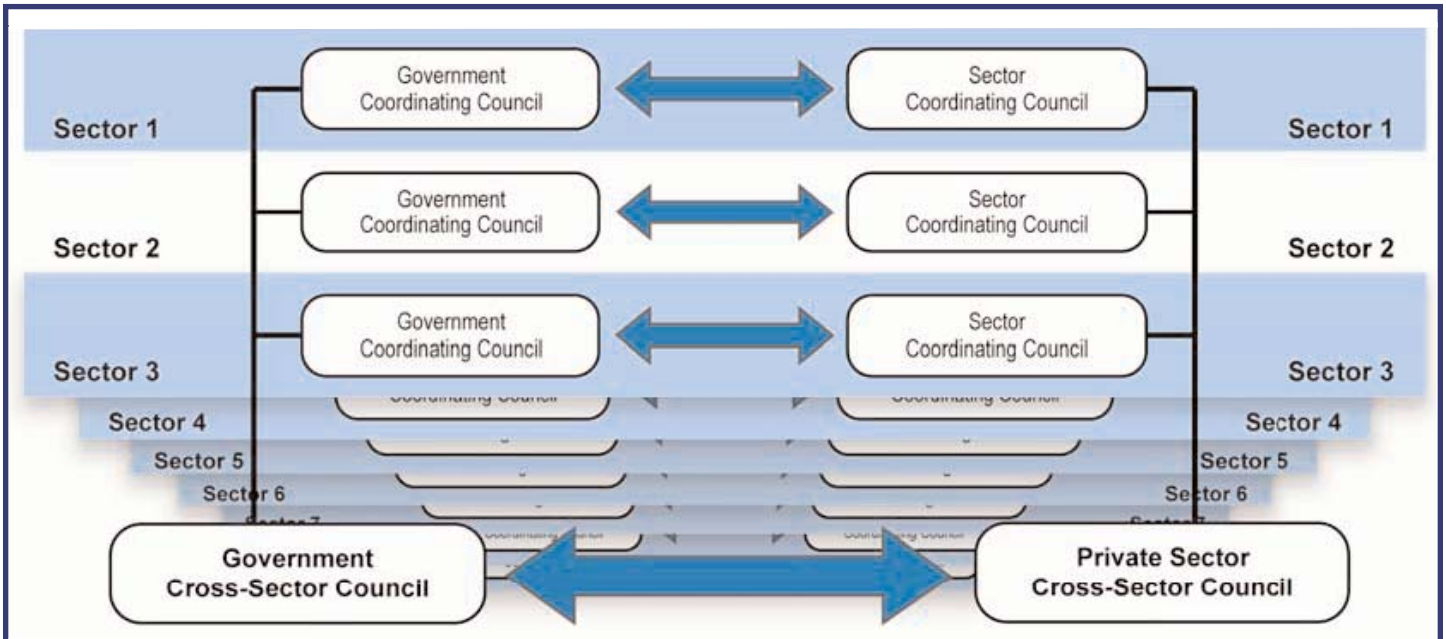
Sector Partnership Model

The National Infrastructure Advisory Council (NIAC) is a body established to provide advice to the Secretary of Homeland Security and the President on the security of information systems for the public and private institutions that constitute the critical infrastructure of our Nation's economy. It is composed of up to 30 members from industry, state and local government, and academia. During the summer of 2005, the NIAC established a Sector Partnership Model Working Group, working from a DHS-requested study on the proposed partnership model, and provided recommendations on the structure, function, and implementation of the model. In October 2005, the Working Group presented its Initial Report and Findings to the NIAC. The Working Group affirmed the structure of the partnership model presented in the Interim NIPP, and made recommendations for key operating principles, including that the partnership be considered a collaboration of equals between the government and the private sector. The Sector Partnership Model Working Group Initial Report and Findings is available online at http://www.dhs.gov/ dhspublic/interweb/assetlibrary/NIAC_SectorPartnershipModelWorkingGroupUpdate_Oct05.pdf.

Sector Level Partnerships

Each of the 17 CI/KR sectors identified in the NIPP has organized, or is in the process of organizing, an SCC to act as a strategy and policy setting body. Some of these councils have existed for many years, such as the Financial Services Sector Coordinating Council, while others are just now forming, such as the Commercial Facilities Sector Coordinating Council. The sector coordinating mechanism, a role envisioned in Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Identification, Prioritization, and Protection, will act much like the designated "sector coordinator" named in 1998 in Presidential Decision Directive (PDD)-63, Protecting America's Critical Infrastructures.

HSPD-7 specifies that DHS and Sector-Specific Agencies (SSAs), such as the Departments of Agriculture, Defense, Energy, Health and Human Services, the Interior, the Treasury, and the Environmental *(Continued, Page 17)*



Sector Partnership Model

Message from PSP Leadership

Kathryn Condello

I am delighted to join the Private Sector Program, and return to the arena of critical infrastructure protection. I had the privilege of being a Sector Coordinator for more than three years, and to support the transition from the earlier PDD-63 environment to the more robust approach reflected in HSPD-7. It is a pleasure to work again with pioneers in this groundbreaking public-private venture, and to participate in building new foundations for the future.

This is the second issue of *The CIP Report* focused on the Private Sector Program, so I would like to take this opportunity to reflect briefly on the accomplishments made over the past year, and look to the challenges ahead.

The Private Sector Program currently supports the Partnership for Critical Infrastructure Security (PCIS) and six Sector Coordinating Councils (SCCs). While the level of provided support varies according to the individual sector's needs, the Private Sector Program's role of coordinating the numerous PCIS and sector meetings, and managing various initiatives on behalf of PCIS and SCC leadership, is valuable to the continual progress of critical infrastructure protection efforts among representatives of private industry. Efforts this calendar year are focused on the completion of individual Sector Specific Plans in accordance with the National Infrastructure Protection Plan (NIPP), increased planning activities associated with pandemic issues, and the implementation of lessons learned following the 2005 hurricane season.

This past year saw numerous changes relevant to public-private partnerships. There was greater recognition, clarification, and formalization of the PCIS and SCC role, stemming from the increased leadership and involvement of the private sector in federal government initiatives surrounding infrastructure protection across the Nation. Further development of the public-private partnership fostered increased information sharing and resulted in significant private sector input into government programs. An example of such input was the thousands of NIPP comments submitted by the private sector, which were then incorporated by DHS into the revised NIPP base plan currently undergoing final review. Joint working groups between *(Continued, Page 11)*

Kathryn Condello manages the Private Sector Program within the Critical Infrastructure Protection Program and is a Principal Research Associate with George Mason University. The Private Sector Program provides analytical, academic, and administrative support related to cross- sector and interdependency issues facing private sector owners and operators of critical infrastructure. This work focuses legal, economic, business, and cultural solutions to enable the private sector to enhance critical infrastructure protection both through private initiatives and working with the government. The Private Sector Program provides assistance to private industry Partnership for Critical Infrastructure Security (PCIS) and Sector Coordinating Councils and provides liaison services between the Department of Homeland Security and the private sector.

Ms. Condello has more than twenty-five years experience in the wireless communications industry and has worked extensively in the Homeland Security, network reliability, and emergency preparedness and response arenas. Ms. Condello served as a Sector Coordinator for the Information and Telecommunications Sector, was a member of the FCC's Network Reliability and Interoperability Council V (NRIC), and was a designated Industry Executive with the National Security Telecommunications Advisory Council (NSTAC).

Ms. Condello has a BA from the University of Virginia and an MBA from Loyola College.

Commercial Facilities Sector Coordinating Council

Renting an apartment, going to the movies, and buying a shirt at the mall - individually or collectively, these events do not give the average person any reason to be concerned. But to the people who own and run these commercial facilities, the safety and well-being of patrons, employees, and structures are on their daily agenda. In October 2005, the Commercial Facilities Sector Coordinating Council (CFSCC) formed with the intention of being a resource to serve the sector's counter-terrorism, security, and emergency response interests. The CFSCC provides DHS and other homeland security partners with an important point of contact to engage participating elements of the Commercial Facilities Sector (CFS) on infrastructure protection issues whenever necessary.

The CFS consists of a wide variety of asset categories including hotels, commercial office buildings, public institutions, casinos, convention centers/stadiums, theme parks, apartment buildings, restaurants, and shopping centers. Since this sector alone encompasses over 100,000 hotels and shopping centers, the CFSCC has been divided into eight sub-councils. Each sub-council has representation on the CFSCC which will allow a better understanding of the industries that make up the entire council. The sub-councils, along with examples of the industries that comprise each sub-council, are listed in the box on this page.

Commercial facilities were identified as key resources in HSPD-7 and the CFS has been formally recognized in the NIPP (Revised Draft NIPP v2.0, January 2006). While responsibility rests with DHS to coordinate with the appropriate departments and agencies to ensure the protection of commercial facilities, which are sometimes referred to as "soft targets", it is quite a challenge. Business is conducted in an especially open manner at these facilities and CFS operates in less of a regulatory environment than most other sectors. With 85 percent of our critical infrastructure and key resources owned and operated by private industry, a great deal of the expertise and resources necessary for instituting better protective measures lies outside the Federal government's control.

Currently, the CFSCC has formed working groups for Communication/Technology and the Sector *(Continued, Page 8)*

Commercial Facilities Sector Sub-Councils and Sample Industries

- Public Assembly Facilities
  - *Movie Theaters*
  - *Convention Centers*
- Sports Leagues
  - *Stadiums*
  - *Arenas*
  - *National Basketball Association (NBA)*
- Resorts
  - *Casinos*
- Lodging
  - *Hotels*
- Outdoor Event Facilities
  - *Amusement Parks*
  - *Fairs*
- Entertainment & Media
  - *Production Studios*
- Real Estate
  - *Office & Industrial Buildings*
  - *Multi-Family Towers & Condos*
- Retail
  - *Shopping Malls*
  - *Retail Centers*

Sports venues, amusement parks, and shopping malls are among the industries that comprise the Commercial Facilities Sector.

Dams, Locks, and Levees Sector Coordinating Council

In May of 2005, the Dams, Locks, and Levees Sector Coordinating Council (DSCC) was formed to act as the private sector interface with the Federal government on issues related to the security of dams, locks, and levees. The DSCC's primary purpose is to determine the nature of the risks posed against dams and related structures so that appropriate and timely information, as well as mitigation strategies, can be provided to those responsible for the operation and protection of these assets.

While the name of the DSCC includes locks and levees, very few, if any, private sector asset owners manage locks or levees; these are primarily under the purview of the Federal government. However, the Gulf Coast hurricanes of 2005 have increased the interest in levees amongst those in the DSCC.

Membership in the DSCC is limited to 25 voting members, and includes U.S. and Canadian non-federal dam owners and operators and representatives from relevant professional associations. The leadership of the DSCC includes a Chair, a Vice-Chair, and a Secretary. Each serves for one year and there are no term limits.

The DSCC does not have an Information Sharing and Analysis Center (ISAC) *per se*, although many of the companies represented in the DSCC are involved with power generation and have access to the Electric and Water ISACs. The DSCC uses the Homeland Security Information Network (HSIN) for information sharing purposes, and is working with DHS to expand HSIN's functions and increase its use in the sector.

Since its inception, the DSCC held four meetings and has formed working groups to evaluate a number of issues, including asset identification, best practices, information sharing, risk assessment methodologies, research and development, and cyber security. Members of the DSCC also reviewed versions 1.0 and 2.0 of the NIPP and individually submitted comments to DHS. ❖

DSCC Member Organizations

Allegheny Energy
Ameren Services Company
American Electric Power
Assn. of State Dam Safety Officials
AVISTA Utilities
Canadian Dam Association
CMS Energy
Dominion Resources
Duke Energy
Exelon
National Hydropower Association
National Mining Association (*ex-officio*)
New York Power Authority
NYC Dept. of Environmental Protection
Pacific Gas & Electric Company
PPL Corporation
Public Utility District #1 of Chelan County
Scana Corporation
South Carolina Public Service Authority
Southern California Edison
Southern Company Generation
TransCanada
U.S. Society of Dams
Xcel Energy Corporation

Oil and Natural Gas Sector Homeland Security Coordinating Council

In late 2004, an audiotape purportedly released by Osama bin Laden called for attacks on Gulf and Iraqi oil facilities. This has since triggered a series of attacks on oil facilities, including the recent attempt by terrorists on the Saudi oil processing facility in Abqaiq, the largest in the world.

Though the attack was thwarted, oil prices spiked amid fears terrorists were targeting critical energy infrastructures. Given the instability of energy markets and the economic impact of terrorist attacks, concerted efforts are being implemented to reduce vulnerability and strengthen resiliency of U.S. oil and natural gas facilities and interests, particularly on the domestic front.

In response to HSPD-7, the Oil and Natural Gas Sector Homeland Security Coordinating Council (ONGSCC) officially formed in the fall of 2004. Consisting of industry trade associations and the owners/operators they represent, the ONGSCC provides a private sector forum for effective communication and coordination of security policies and strategies within the sector. Enhancing lines of communication allows the ONGSCC to engage and inform the private sector of infrastructure protection issues while providing a single point of contact for the government regarding sector security.

Besides the threats posed by terrorism, the ONGSCC is also working to improve preparation and mitigation *(Continued, Page 14)*

Food and Agriculture Sector Coordinating Council

The Food and Agriculture Sector Coordinating Council (FASCC) is comprised of 21 representatives from the Food and Agriculture Sector. The self-governing body represents the Food and Agriculture Sector to the government and makes policy and strategy recommendations to the Federal government. The 21 representatives are elected by seven sub-councils. The FASCC meets quarterly with the Government Coordinating Council (GCC) and members regularly meet with one another in other capacities.

Following the most recent FASCC-GCC joint session, held January 24, 2006, a new meeting schedule was introduced. In place of the previously held quarterly meetings, the sector will now conduct two tabletop exercises per year and hold two quarterly joint sessions. These exercises are meant to encompass the decision-making process, communication, and coordination of multiple agencies and the private sector. The next 2006 meeting will be a tabletop exercise targeting bottled water, to be held in North Carolina.

The sector continues to be very active in other areas as well. The group recently finalized their 2006 goals, which include:

- Enhance and improve two-way communication;
- Establish emergency food distribution and feeding corps;
- Conduct tabletop exercises with sector; and
- Establish understanding of what constitutes an asset structure for agriculture and food systems.

In addition, the private sector is participating in a variety of activities both independently and in partnership with the government. Among these are Strategic Partnership Program Agroterrorism (SPPA) assessments in partnership with the Food and Drug Administration (FDA) and Department of Agriculture (USDA), review of the NIPP in partnership with DHS, and introduction of programs such as OK 4-72, an awareness campaign on disaster preparedness within the industry.

For more information, the FASCC can be contacted at FASCC@gmu.edu. ❖

Water Sector Coordinating Council

The Water Sector Coordinating Council (WSCC) was formed in September of 2004 and serves as a policy, strategy, and coordination mechanism which recommends actions to reduce and eliminate significant homeland security vulnerabilities to the water sector, including drinking water and waste water treatment, through interactions with the Federal government and other critical infrastructure sectors.

Membership in the WSCC is limited to 16 voting members, representing privately- and municipally-owned water and waste water utilities, and eight non-voting members, representing professional water and waste water associations, who appoint the voting members. The WSCC is led by a Chair and a Vice-Chair.

Since its inception, the WSCC has met on a number of occasions and has considered many important issues, including the NIPP, the Sector Specific Plan (SSP), the National Asset Database (NADB), the Homeland Security Information Network (HSIN) and the Water Information Sharing and Analysis Center (ISAC), the Protected Critical Infrastructure Information (PCII) Program, the National Drinking Water Advisory Council's Water Sector recommendations concerning active and effective security programs for water utilities, and the Environmental Protection Agency's Water System Security Research Action Plan. Looking ahead, the WSCC is anticipating issuance of the final NIPP base plan and development of the sector's SSP. ❖

Commercial Facilities *(Cont. from Page 5)* Specific Plan as input to the NIPP. These working groups meet on an as needed basis, as does the sector as a whole. The Private Sector Program will facilitate meetings and provide executive secretariat support to the council as it goes forth in its endeavor to address the critical infrastructure protection issues of its members. ❖

WSCC Member Organizations

Associations:

- American Water Works Association (AWWA)
- Association of Metropolitan Water Agencies (AMWA)
- Awwa Research Foundation (AwwaRF)
- National Association of Clean Water Agencies (NACWA)
- National Association of Water Companies (NAWC)
- National Rural Water Association (NRWA)
- Water Environment Federation (WEF)
- Water Environment Research Foundation (WERF)

Utility Members:

- Alexandria Sanitation Authority
- American Water Works Service Company
- Bean Blossom Patricksburg Water Corporation
- Boston Water and Sewer Commission
- Breezy Hill Water and Sewer Company
- City of Portland Bureau of Environmental Services
- City of Richmond Department of Public Utilities
- Columbus Water Works
- East Bay Municipal Utility District
- Fairfax Water
- Greenville Water System
- Los Angeles Dept. of Water and Light
- Manchester Water Works
- New York City Department of Environmental Protection
- Pima County Wastewater Management Department
- United Water Management & Service Company

Legal Insights

Expressa nocent, non expressa non nocent.

Things expressed do harm; things not expressed do not.

Brett Callahan, CIP Program Legal Intern

They teach you in law school not to volunteer information. Giving away too much tips your hand and can get you and your client into trouble. The private sector currently faces a similar dilemma: sharing information with DHS is necessary to effectively protect the private sector and the country at large, but in doing so, private sector entities may give competitors an advantage, open themselves to liability, and in fact make themselves more vulnerable to terrorists. DHS and the private sector are trying to strike a delicate balance and the process is potentially frustrating.

It is important to recognize the plethora of barriers to full disclosure by the private sector. Various open-government laws like the Freedom of Information Act (FOIA) and the Federal Advisory Committee Act (FACA) make the private sector wary of turning over information to the government. Public accessibility of information makes a better government, but is bad for business. While there are exemptions to FOIA and FACA for some normally confidential information like trade secrets and commercial and financial information,[1] these exceptions do not provide the protections the private sector might want.

Congress recognized this problem when drafting the Homeland Security Act of 2002 (HSA). Much of the testimony and floor debate focused on how to balance the government transparency that is necessary for democracy to flourish while providing the private sector with enough protection for private sector individuals and entities to be comfortable coming forward with necessary information. Programs like the Protected Critical Infrastructure Information (PCII) Program provide broader protection from FOIA disclosure than the exemptions included within FOIA itself.

Congress also created a concise, but potentially very powerful, provision when it drafted the statute empowering the Secretary of Homeland Security to create advisory committees.[2] § 871 of the HSA allows the Secretary to exempt any DHS advisory committee from complying with FACA.

FACA requires timely notice of meetings, meetings open to the public, and public accessibility of documents. If an advisory committee will be discussing a topic that falls within a FACA exception, the committee must provide timely notice of its intent to hold a closed meeting and case law makes clear that only the part of the meeting dealing with an exempted topic may be closed. If a committee falls under FACA, failure to comply fully with its requirements can be severe. Courts have ordered non-compliant advisory committees to disclose documents and minutes of past meetings, enjoined committees from meeting again until they were in compliance, and in extreme cases, enjoined the

"It is apparent that [FACA] contains a very broad, imprecise definition, and in this respect is not a model of draftsmanship."

Judge Gerhard Gesell

(Continued, Page 10)

Legal Insights *(Cont. from Page 9)* use of non-compliant advisory committee reports in policy formulations.

Uncertainty over how to interpret FACA's terms has spawned significant litigation and it seems as if the meaning of nearly every word in the statute has been debated in court. When a dispute involving the implication of the word "utilize" arrived before the Supreme Court, the Court scrapped the plain meaning of the term because "'utilize' is a wooly verb" and instead created a two-part test for when a committee is "utilized" under the statute.[3] Because the terms of FACA are unclear it can be easy to accidentally violate the statute and only find out the committee is not in compliance with FACA in court.

Since the risk of litigation is high when FACA is involved, it is understandable that the private sector would want nothing to do with FACA. Costs may outweigh benefits for the private sector to exchange information with DHS under FACA; the expense of litigation is high and the private sector must combine litigation costs with the possibility of losing in court and having sensitive information exposed. As such the § 871 exemption is a powerful tool. It allows the private sector to bypass many barriers to discourse with DHS and over all reduces the burden on the private sector making the free flow of information much more likely.

Many groups have recommended the Secretary invoke the FACA exemption. It should, however, be noted § 871 has some political controversy attached to it. Some critics do not like the idea of a statute designed to allow groups to circumvent open government laws designed to enforce accountability and increase public trust in the government.

Just recently Secretary Chertoff decided to invoke the § 871 FACA exemption for the Critical Infrastructure Partnership Advisory Council (CIPAC).[4] CIPAC will consist of members of the various private sector Sector Coordinating Councils and Federal, state, local, and tribal government representatives from the Government Coordinating Councils.

In invoking the FACA exemption, Secretary Chertoff recognized the competing interests between full and open disclosure by the private sector to the government and full and open disclosure by the government to the people. In creating CIPAC, DHS tried to strike a balance. Although Secretary Chertoff exempted CIPAC from FACA, CIPAC will still comply with the spirit of FACA. CIPAC will maintain a public website with as much information posted as is reasonable. Additionally, they will provide public notice of meetings when reasonable, and when there are no conflicting security concerns.

Essentially, it appears DHS is using the FACA exemption, not as a shield to government openness, but as a way to make it a little bit easier for the private sector to share information with the government and allay some of their fears about litigation. For example, the FACA exemption will make it easier for meetings to be held on short notice. However, it is likely the biggest benefit will be protection from litigation. Most of the meetings CIPAC closes would likely be permissible to close under regular FACA exceptions. It is also probable that documents CIPAC withholds would be permissible to withhold under regular FACA exceptions. However, invoking the § 871 FACA exemption protects CIPAC from ever having to engage in FACA litigation in the first place. It also protects CIPAC from being forced to disclose information when it almost, but not quite complied with FACA. As noted above, FACA is confusing and it is easy to accidentally violate one of its provisions.

DHS found a good equilibrium in how it choose to invoke the § 871 FACA exemption. The exemption will encourage the private sector to volunteer critical information while minimizing their fear they may compromise business in doing so. However, it does not totally cut the public off from information the public needs to hold the government accountable. ❖

[1] 5 U.S.C. 552(b)(4).
[2] 6 U.S.C. 451.
[3] *Public Citizen v. United States Dep't of Justice*, 491 U.S. 440.
[4] 71 F.R. 14930 (March 24, 2006).

DHS Office of Infrastructure Protection Launches Security Awareness Campaign

The Department of Homeland Security has launched a security awareness campaign, *Protect Your Workplace*, to provide guidance on how to make the workplace a more secure environment and how to report suspicious behavior, activity, and cyber incidents. The campaign makes posters and a brochure available to all businesses as a resource for protecting the workplace. Materials are available for download at www.us-cert.gov/reading_room/distributable.html.

Private Sector Program *(Cont. from Page 4)* the sectors and their government counterparts have produced fruitful outcomes in addressing policy and strategic concerns. Improved communication and expanded information sharing mechanisms assisted in promoting the public-private partnership and paving the way for future collaboration.

As PCIS and the SCCs continue work to strengthen private sector critical infrastructure protection, further collaboration with the Federal government will address both existing and emerging homeland security challenges. The private sector will have the opportunity to exercise sector-specific and cross-sector planning mechanisms under the auspices of pandemic planning. The private sector's work in this field will complement the efforts of the Federal government and lead to a better understanding of specific private sector needs, concerns, and interdependencies. Moreover, as the Federal government moves to implement lessons learned from the hurricanes of 2005, the private sector is also exploring best practices and recommendations to address within industry. Improving incident response plans and building upon preparation efforts will prove beneficial not only to private industry, but also to the public sector and general community. Ultimately, it is with strong private sector involvement and the leveraging of the sectors' own subject-matter expertise that we can meet the challenges that lie ahead in advancing our Nation's security. ❖

PCII Program Marks Two Years of Helping DHS, Industry Protect National Infrastructure

February 2006 marks the two-year anniversary of the Protected Critical Infrastructure Information (PCII) Program. The PCII Program, part of the Department of Homeland Security (DHS), facilitates secure information sharing between the private sector and government about the crucial systems, networks, and facilities that support the nation's day-to-day operations.

Private industry owns and controls 85 percent of the nation's critical infrastructure, such as railroads, power lines, hospitals, farms, communications, and financial networks. DHS needed a way to access information about these indispensable systems and facilities to better assess security risks and recovery measures. The PCII Program, which commenced operation on February 18, 2004, was designed to encourage the private sector to voluntarily share critical infrastructure information by offering special protection from public disclosure to this important and sensitive information.

In the past six months alone, private sector submissions of critical infrastructure information have quadrupled. "PCII has come a very long way," said Laura Kimberly, PCII Program Manager. "The program has significantly evolved over the past 24 months, but more importantly, it has established new and growing relationships that open fresh avenues for information sharing."

Kimberly and the program staff are excited about seeing the government and private sector continue to strengthen their information-sharing relationships. "The people of this program have spent hours bringing industry and government together," she said, "and now we can see those relationships evolve into information-sharing partnerships that will make our homeland more secure."

The PCII Program was created under the Critical Infrastructure Information Act of 2002 to enable those with knowledge of critical infrastructure to voluntarily share sensitive information by protecting it from public release under the Freedom of Information Act, state and local open records laws, and use in civil litigation.

Kimberly said getting the private sector to submit information is not always easy. "Like anything new, it takes time to build up people's trust - we are dedicating ourselves to reaching out to industry," said Kimberly. "And now we are beginning to see the fruits of our labor."

Submissions have increased tenfold in the past year.

Reaching Out to Industry

The PCII Program Office has publicized the program at numerous conferences to reach out to individual industry sectors, and hosted discussions with private sector and government representatives to determine the best approach to effective information sharing.

Kimberly credits the growth of the program to its training and safeguarding procedures that increase security and build confidence among private sector submitters. Moreover, the PCII Program Office developed new ways to make it easier for private industry and their government partners to communicate and share information.

In 2005, the program began accepting submissions electronically. Critical infrastructure information can now be submitted through a secure portal accessed from the PCII Program Web site at www.dhs.gov/pcii.
(Continued, Page 14)

GMU's Technology Management Program Joins Forces with DHS to Empower Executives & Strengthen National Security

Forty-five students in the George Mason University Master of Science in Technology Management Program (MSTM) kicked off a new DHS pilot program to help assure that current and future executives across the Nation are prepared to meet the major security and emergency preparedness challenges faced by U.S. businesses and government. The program will be expanded to include George Mason Executive MBA students later this year.

The pilot program is aimed at facilitating the incorporation of business continuity planning and security topics into graduate business school programs. The purpose is to develop improved awareness, understanding, and investment in protective security strategies by establishing partnerships with universities to better prepare the Nation's future leaders to plan, implement, and manage protective measures and business continuity planning for private sector critical infrastructure.

For the next eighteen months, the DHS initiative will involve the George Mason technology management graduate students in simulations, lectures, and discussions of major business continuity issues. The program will address critical issues including cyber-security, physical infrastructure security, emergency preparedness, and the role of the private sector in developing related procedures, products, and services. Students will also receive reference materials to supplement their class work and assist them on the job.

"In light of events such as September 11 and Hurricane Katrina, we have all become intensely aware that information systems and networks are of ever-increasing importance to business and government success and indeed enable business and government to operate," said Richard J. Klimoski, Dean, George Mason University School of Management. "The nation's current and future technology leadership must be prepared to act and equipped to lead in an era of major security and business continuity challenges."

Speakers for the first DHS session on the George Mason campus featured Wade Townsend, Chief, Program Support Branch of the Risk Management Division of the Office of Infrastructure Protection at DHS, Jim McDonnell, President, McDonnell Consulting Group, and David Howe, Managing Director and COO, Civitas and previously Special Assistant to the President and Senior Director for Emergency Preparedness and Response at the Homeland Security Council at the White House. Future guest speakers will include leading government officials and private sector executives, as well as experts on homeland and national security policies, technical and physical infrastructure security, and overall emergency preparedness.

"Incorporating security and business-continuity planning concepts into the programs that make up the system that produces today's and tomorrow's managers is paramount in maintaining and increasing the resiliency of America's economy and critical infrastructure," said Justin Taft of Systems Planning and Analysis, Inc., a consulting firm working with DHS to implement the program with graduate-level business students across the country.

Cameron Jordan, MSTM Class of 2007 and senior systems engineer at Raytheon, echoed the feeling of many participating students: "The DHS pilot advances our expertise as managers and executives. We are all facing choices in our professional lives regarding risk assessment, security investment, and emergency preparedness. The opportunity to hear leading experts and policy makers, and gain hands-on experience through real world simulations, better prepares us to make these choices in a wise and informed manner. Not only will we be helping our organizations, but our country as well." ❖

PCII *(Cont. from Page 12)*
The PCII Program is deploying its expertise and experience in facilitating information sharing to enhance current and future homeland security efforts. The PCII Program recently partnered with DHS's Risk Management Division for the Chemical Comprehensive Review, an interagency project that will conduct site visits to chemical facilities in select cities and regions and gather security information. Facilities will have the option of seeking PCII protection for the information they submit during the process.

Reaching to First Responders

The program is developing relationships with state and local government entities to speed access to PCII for first responders and other state and local homeland security personnel. Collaboration with state and local officials is yet another way that private industry and government will grow a stronger and more trusting relationship.

Maryland was the first state to be accredited under the PCII Accreditation Program, which allows a state or agency to have access to PCII. The PCII Program will be collaborating with Maryland officials and first responders to increase the amount of private sector critical infrastructure information available to Maryland and Federal homeland security personnel. Discussions to create similar information-sharing programs are also in progress with other states.

In California, through Project Constellation, DHS and the PCII Program are cooperating with the City and County of Los Angeles to develop multi-agency prevention and response management initiatives for critical locations in the Los Angeles area. The data submitted will be made available to local law enforcement and emergency personnel in the event of an emergency. The Los Angeles pilot will be expanded to the State of California beginning in March.

In 2005, the PCII Program Office partnered with the New York State Office of Homeland Security to collect security-related information about chemical facilities in the state. Respondents to a state-led inquiry were able to make submissions of PCII to DHS from the same web portal that served to collect information for homeland security personnel in New York State. The information gathered can be used by both New York State and DHS to improve analysis of threats and vulnerabilities.

"The PCII Program Office's role has evolved from one that stores and disseminates CII to one that creates bridges between the private sector and the government - making it easier for information to be shared," said Kimberly.

For more information, contact the PCII Program Office at (202) 360-3023 or visit www.dhs.gov/pcii. ❖

Oil and Natural Gas *(Cont. from Page 7)* procedures for natural disasters such as the 2005 hurricanes that devastated the Gulf Coast and halted many sector operations. Working groups within the Council have been formed. The Homeland Security Information Network (HSIN) Working Group is making continued efforts to get the ONG HSIN portal up and running. The HSIN portal provides the sector with real-time updates and alerts and is a successor to the Energy Information Sharing and Analysis Center (ISAC).

The Council has also formed the NIPP Working Group to examine the Sector Specific Plan (SSP) and will work closely with the Department of Energy in the development of this plan. The CIP Program's Private Sector Program provides secretariat support to facilitate coordination between the ONGSCC and its government counterparts. ❖

GEORGE MASON UNIVERSITY | School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

You are cordially invited to...

A panel on the

Committee on Foreign Investment in the United States (CFIUS)

The panel features authors from the Critical Infrastructure Protection Program's February 2006, Monograph on CFIUS. Panelists will discuss legal issues regarding foreign direct investment and legislative challenges to CFIUS.

Panelists include:

Dr. Edward M. Graham
Senior Fellow, Institute for International Economics
David Marchick, Esq.
Covington & Burling
The Hon. Patrick Mulloy
Commissioner, United States-China Economic and Security Review Commission
Kristen Verderame, Esq.
Chief Counsel, BT Americas and VP, Commercial, Legal & Regulatory BT Global Services

Moderator:

Prof. William Lash, III
Professor of Law, GMU School of Law
Former Assistant Secretary for Market Access and Compliance for the Department of Commerce

Lunch will be offered with a keynote speech by:

Stewart A. Baker, Esq.
Assistant Secretary for Policy for the Department of Homeland Security

Friday, April 28, 2006

Continental Breakfast: 8:30 - 9:30 a.m.
Welcome: 9:30 - 9:45 a.m.
Panel Discussion & Questions/Answers: 9:45 - 12:00 p.m.
Lunch Keynote Speaker: 12:00 - 1:30 p.m.

George Mason University School of Law
3301 Fairfax Dr. Arlington, VA 22201

R.S.V.P. Amy Cobb
(703) 993-8193 or acobb1@gmu.edu
Please note that seating is limited.

GEORGE MASON UNIVERSITY | School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

MERCATUS CENTER
GEORGE MASON UNIVERSITY

Paperwork Reduction Act - 25th Anniversary Event Invitation

Dinner Reception

June 16, 2006

The Atrium
George Mason University School of Law
Hazel Hall
3301 Fairfax Drive
Arlington, VA 22201

The Critical Infrastructure Protection Program (CIPP) at George Mason University School of Law and the Mercatus Center at George Mason University cordially invite you to celebrate and reflect on the 25th Anniversary of the Paperwork Reduction Act (PRA) and the establishment by Congress of the Office of Information and Regulatory Affairs (OIRA). Our celebration will begin with a reception at 5:30 p.m. followed by guest speakers' remarks and dinner.

Over the past 25 years, the PRA has influenced Congressional and Executive involvement with critical issues in regulation, information, and technology management facing the federal government and the public. Our kick-off panel discussion will explore the legacy of the PRA, the evolution of regulatory and information oversight, and its continued relevance as new information and regulatory challenges emerge.

Registration: Please RSVP by May 12, 2006 to Amy Cobb, GMU CIPP, Tel: (703) 993-8193 or via email acobb1@gmu.edu.

PSP Overview *(Cont. from Page 3)* Protection Agency, "shall collaborate with the private sector and continue to support sector-coordinating mechanisms:

(a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and

(b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."

The SSAs, DHS, and other related Federal and state agencies formed GCCs to serve as counterparts to the private sector SCCs. For each CI/KR sector, the two groups meet together to coordinate activities, plans, and to share information. With the private sector's input, these bodies are making recommendations to foster the most beneficial public-private relationship with DHS and SSAs.

Cross-Sector Coordination

A cross-sector coordinating council was established to address common and cross-sector concerns of the private sector, and to serve as the key private sector group for providing input into the development of the NIPP. The Partnership for Critical Infrastructure Security (PCIS) formed in 2000 and was comprised initially of designated Sector Coordinators, a role identified in 1998 in PDD-63. Subsequently, PCIS reorganized to align itself with the new roles of the sector coordinating mechanism envisioned in HSPD-7, and has been serving as the cross-sector coordinating council. Membership of the cross-sector group consists of chairs of the SCCs, with the chairs of new SCCs able to gain a seat on PCIS once established. PCIS serves as a valuable resource to DHS and the SSAs, giving the federal government insight on private sector issues and concerns. Related to NIPP development and implementation, PCIS provided input to DHS on a number of issues that affected many sectors, including information sharing, physical and cyber security, and research and development.

PSP currently provides secretariat support, to include facilitation and coordination of sector matters, to the Private Sector Cross-Sector Coordinating Council, PCIS, and the following SCCs: Commercial Facilities; Dams, Locks, and Levees; Food and Agriculture; Healthcare; Oil and Natural Gas (a sub-sector of Energy); and Water. PSP also acts as a liaison between the government and the SCCs and the Private Sector Cross-Sector Coordinating Council. By acting as a cross-sector coordinator and facilitator, the CIP Program at George Mason University School of Law is exposed to many issues common to the various sectors and can act as a liaison between the private sector, government, and PSP among the various sectors. This exposure enables the CIP Program to provide a big picture view to specific sectors and also provide insight into the evolving needs of both the private sector and government. ❖

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.