The Critical Infrastructure Protection Program April 2005 / Volume 3, No. 9

THE CIP REPORT

The CIP Private Sector Program

Newsletter Editorial Staff

John McCarthy, *Director / Principal Investigator*

Jessica M. Milloy, *Special Assistant to the Director*

Amy Cobb, *Senior Project Associate*

Jeanne Geers, *CIP Report 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.

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Building on previous experience and expertise, the CIP Program began providing secretariat facilitation and assistance to private industry Sector Coordinators, Information Sharing and Analysis Centers and other groups with respect to Homeland Security issues in December of 2003. As this support grew, the CIP Program was excited to welcome Rod Nydam to the CIPP staff in the formation of the Private Sector Program (PSP) in April of 2004. 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 and helps manage the interface with appropriate Department of Homeland Security program elements. This work focuses on 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. Recognizing the need for and value of these initiatives, the Federal government, through the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, provides funding to the Private Sector Programs.

Private Sector Programs has grown at an enormous rate, now providing coordination for three sectors, and anticipating a fourth sector. This issue of *The CIP Report* highlights the complexities of each sector, while providing more information on cross sector coordination and issues facing the private sector.

Additionally, we have the second of three symposium events focusing on federal-level cyber security compliance scheduled for April 26, with more registration information included in this issue. Also included in this issue is registration information for our roundtable dialogue of lessons learned regarding IT Security and Sarbanes Oxley Compliance scheduled for May 3 at the Ronald Reagan Building in Washington, D.C.. Finally, we also include 'Save the Date' information for our next Critical Conversation, focusing on Cyber Security, which will be held at the National Press Club on May 18. For more information on any of these events, please contact Amy Cobb of the CIP Program, (acobb1@gmu.edu).

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

Private Sector Program Overview and Cross-Sector Organization

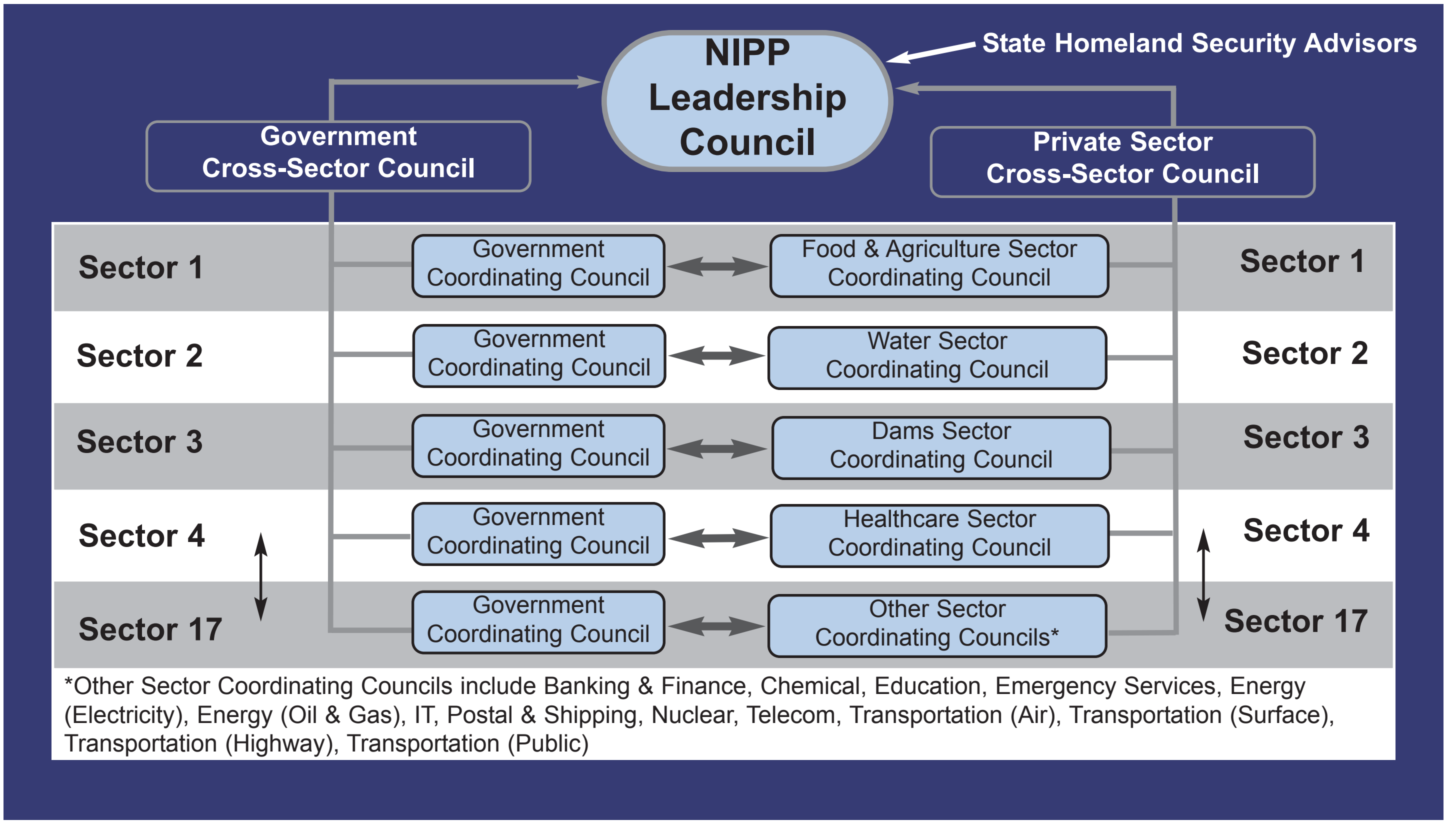
Using the broad base of knowledge developed by the CIP Program, the Private Sector Program focuses its activities on industry's role in protecting critical infrastructure. "Private Sector," as used in this description, essentially means owners and operators of facilities, whether purely privately owned, such as an oil refinery or a railroad, or publicly owned facilities such as a municipal or state run water utility.

The Private Sector Program currently manages the following key projects: (i) facilitation and coordination of the Private Sector Cross Sector Coordinating Council which is the primary group providing private sector and operating entities' input into the National Infrastructure Protection Plan (NIPP) implementation; (ii) coordination of the water sector; (iii) coordination of the food and agricultural sector coordinating council; (iv) anticipated coordination of the dams, locks and levees sector; and, (v) anticipated coordination of the healthcare sector. The Private Sector Program also acts as a liaison between the government and private sector coordinating councils and the private sector cross sector coordinating council.

Cross Sector Facilitation and Coordination

The Private Sector Cross Sector Coordinating Council was established to address common and cross sector concerns of the private sector as well as being the key private sector group for input into the NIPP implementation. It is anticipated that the Partnerships for Critical Infrastructure Security, Inc. (PCIS) will act as the cross sector group. PCIS was formed in 2000 with designated Sector Coordinators, a role identified in 1998 by Presidential Decision Directive - 63 "Critical Infrastructure Protection." Today, PCIS has been reorganized to accommodate the sector coordinating council regime under HSPD-7.

The chart below indicates the relationship between this group, the government and the other sector coordinating councils. By acting as the cross sector coordinator and facilitator, GMU is exposed to many issues common to the various sectors and can act as a liaison both between the private sector and the government and *(Continued, Page 3)*


NIPP Leadership Council
State Homeland Security Advisors
Government Cross-Sector Council
Private Sector Cross-Sector Council
Sector 1
Government Coordinating Council
Food & Agriculture Sector Coordinating Council
Sector 1
Sector 2
Government Coordinating Council
Water Sector Coordinating Council
Sector 2
Sector 3
Government Coordinating Council
Dams Sector Coordinating Council
Sector 3
Sector 4
Government Coordinating Council
Healthcare Sector Coordinating Council
Sector 4
Sector 17
Government Coordinating Council
Other Sector Coordinating Councils*
Sector 17

*Other Sector Coordinating Councils include Banking & Finance, Chemical, Education, Emergency Services, Energy (Electricity), Energy (Oil & Gas), IT, Postal & Shipping, Nuclear, Telecom, Transportation (Air), Transportation (Surface), Transportation (Highway), Transportation (Public)

Rod Nydam, J.D. is an Associate Director of the Critical Infrastructure Protection Program at George Mason School of Law and manages the Private Sector Programs project which includes providing analytical, academic and administrative support related to cross sector and interdependency issues related to the 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.

Prior to joining GMU Law School, Rod was a corporate attorney for 17 years as a partner at Howrey & Simon LLP and McGuireWoods LLP. He focused on corporate governance, mergers & acquisitions, international, security and regulatory matters. Rod has a B.A. in Economics from Cornell University and a J.D. from Cornell Law School.

Private Sector Program *(Cont. from Page 2)* among the various sectors. This exposure enables GMU to provide a big picture view to specific sectors and also provide insight into the needs of both the private sector and government.

Related to NIPP implementation, the cross-sector group is actively working with DHS on a number of issues that affect many sectors, including research and development. The cross sector coordinating council identified a need to convene R&D professionals from the private sector and have a discussion with DHS and other federal agencies on the priorities for critical infrastructure R&D in the nation. This workshop is expected to be the beginning of a series of dialogues related to R&D.

Specific Sector Coordinating Councils

Each critical infrastructure sector in the private sector is organizing a sector coordinating mechanism that reflects the make up of the natural sector structures and will 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. The sector coordinating mechanism, a role recognized in Homeland Security Presidential Directive-7 (HSPD-7), will act much like the designated "sector coordinator" role that has been in place since 1998 with the Presidential Decision Directive - 63, and will focus on broader representation within each sector.

HSPD-7 specifies that the Department of Homeland Security and Sector-Specific Agencies (DOD, DOE, DOI, EPA, HHS, Treasury, USDA, etc.) "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."

Private Sector Programs provides coordination of the Food and Agriculture sector, Water sector, Dams, Locks, and Levees sector, and the Healthcare sector. PSP assists the sector coordinating councils' work with the overall Cross Sector Coordinating Council. With the private sector's input, these bodies will make recommendations to foster the most beneficial public private relationship with the Department of Homeland Security and Sector-Specific Agencies. A description of these sectors and their work for critical infrastructure protection is outlined in the subsequent articles of this edition of *The CIP Report.* ❖

Seeing Eye to Eye on Security from Farm to Table: Food and Agriculture Sector

The CEO of a major fast food chain may have little in common with a Nebraska corn farmer. Yet, the responsibility to safeguard the nation's supply of food and agriculture lie heavily on both of them. Prior to the 9/11 attacks, al-Qaeda operatives in the United States studied crop-spraying airplanes in addition to passenger jets. In late March of this year, US intelligence confirmed that Osama bin Laden was attempting to recruit Abu Mousab al-Zarqawi, the man alleged to mastermind many of the beheadings in Iraq, to attack on U.S. soil. One of al-Zarqawi's aides stated during an interrogation that al-Zarqawi has set his sight on soft targets (restaurants, schools, and movie theaters). Though no official ties can be linked between al Qaeda and Russia's tragedy at Beslan, the event indicates that soft targets could be a very real target in modern terrorist strategy.

Couple this with the recent GAO report discussing the potential vulnerability of the nation's cattle supply[1] and the report issued by the Harvard School of Public Health and four other institutions stating that an attack on the nation's rural areas can have serious and reverberating consequences[2], all of a sudden the fast food chain CEO and the Nebraska farmer seem more closely tied than before. Joining them at the security roundtable are numerous federal, state and local government officials.

In December 2004, the CIP Program began detailed efforts with the newly formed Food and Agricultural Sector Coordinating Council (FASCC). DHS requested GMU to serve as the facilitator, coordinator, and secretariat for the FASCC and its seven subcouncils. The FASCC is comprised of 21 organizations, each appointing an individual to represent associations and Owners/Operators in the private sector portion of the Food and Agriculture sector. The self-governing body *(Continued, Page 6)*

Expanding the Healthcare and Public Health Sector Coordinating Council

Bioterrorist threats, epidemics, security, and rising healthcare costs are just some of the challenges facing the National Healthcare and Public Health Sector. Congress has already responded to these ongoing concerns with the introduction of the Public Health Preparedness Workforce Act of 2005 (S.506). Sponsored by Senators Chuck Hagel (R-NE) and Richard Durbin (D-IL), this legislation will ensure an ample supply of healthcare providers to confront terrorist acts, natural disasters, infectious diseases and more.

As with some other critical infrastructure sectors, the Healthcare sector is expanding to include many aspects of the industry. The current Healthcare Sector Coordinating Council, recognized in 2003 under PDD-63 by then Secretary of Health and Human Services Tommy Thompson, has representation from hospitals and other companies such as Blue Cross/Blue shield, GE Medical Systems, Pfizer, and the American Medical Association. After the new Healthcare and Public Health Sector Coordinating Council forms or reorganizes, Private Sector Programs plans to facilitate meetings and provide executive secretariat support to the council as it forms policy and sets a strategy for securing the sector.

The newly expanded council is expected to have many strategic goals for protecting the sector's infrastructure to ensure healthcare delivery that is essential to the security and well-being of the nation. As with other sector coordinating councils in other CIP sectors, the Healthcare and Public Health Sector Coordinating Council will act as a voice for the industry in working with Federal, State and local governments on infrastructure protection issues. In this effort the healthcare sector will partner with the government and other critical *(Continued, Page 7)*

Water Sector Coordinating Council

Utility Members

Alexandria Sanitation Authority
American Water Resources Company
Bean Blossom Patricksburg Water Corporation
Boston Water and Sewer Commission
Breezy Hill Water & Sewer Company
Bureau of Environmental Services
City of Phoenix, Water Services Department
City of Portland, Oregon Bureau of Environmental Services Wastewater Group Operations and Maintenance Division
City of Richmond Department of Public Utilities
Cleveland Division of Water
Columbus Water Works
Greenville Water System (Chair)
Manchester Water Works Water Treatment Plant
New York City Department of Environmental Protection (Vice Chair)
United Water Management & Service Company
Water Services, Los Angeles Department of Water & Power

Association Members

American Water Works Association
Association of Metropolitan Sewerage Agencies
Association of Metropolitan Water Agencies
AWWA Research Foundation
National Rural Water Association
National Association of Water Companies
Water Environment Federation
Water Environment Research Foundation

Water Sector Coordinating Council Overview

In September 2004, the Water sector was reorganized into a sector coordinating council and has been meeting regularly to address critical infrastructure protection issues for the owners and operators of water and wastewater systems across the nation. The members of the council represent the natural breakdown of systems that exist in the Water sector including: water and wastewater, urban and rural, public and private, and the eight associations and research foundations that exist in the sector. The membership list of the Water Sector Coordinating Council (WSCC) can be found in the sidebar.

The concepts for forming the council were agreed upon by the eight water/wastewater associations and research foundations last summer. The CIP Program became the executive secretariat for the council and facilitated the council formation in September and subsequent meetings for the group. The WSCC established their mission in September 2004:

The Water Sector Coordinating Council serves as a policy, strategy and coordination mechanism and recommends actions to reduce and eliminate significant security vulnerabilities to the water sector through interactions with the Federal Government and other critical infrastructure sectors.

The WSCC formed working groups to address some early issues including information sharing within the sector and with the government, and research and development for security. The information sharing working group is looking at models of existing and proposed mechanisms to ensure that sector needs are addressed and information and analysis that exists in the sector and at the federal government level are shared in a true public-private partnership.

The water sector has been active in homeland security before the WSCC was formed; under PDD-63, the Association of Metropolitan Water Agencies represented the sector in the cross sector group, the Partnership for Critical Infrastructure Security, Inc. (PCIS), and also established the Water Information Sharing and Analysis Center (WaterISAC) in 2001. With guidance from an advisory group of utilities and the other associations, the WaterISAC was created to improve security by facilitating the sharing and analysis of information in the sector. Today the WaterISAC also sponsors a free service called the Water Security Channel (WaterSC), designed to disseminate U.S. EPA and Department of Homeland Security advisories by e-mail to all drinking water and wastewater systems and to state agencies. In addition, the DHS is sponsoring an information sharing

(Continued, Page 8)

LEGAL INSIGHTS

by Rod Nydam

PCII, CII and Other Legal Issues

Given years of exposure to public - private sector information sharing issues, several recurring issues present themselves. PSP is working on a practicality based legal and economic analysis of issues which present hurdles to information. From time to time, PSP will be publishing detailed analysis of some of the legal hurdles to information sharing. The discussion below highlights two of the items that will be discussed in the future.

Strengthen the Protections of the CII and PCII Program.

DHS set up the Protected Critical Infrastructure Information (PCII) Program to encourage the private sector to share sensitive and proprietary business information about critical infrastructure with the federal government. Members of the private sector can voluntarily submit sensitive information to DHS with the understanding that DHS will protect the information from disclosure, assuming all the requirements of the Critical Infrastructure Information Act of 2002 have been met. The regulations for the PCII program are very strict and require a specific request as well as additional information to justify keeping any shared information out of the public view.

Using feedback from private industry and drawing on the legal expertise within the program, the PSP has identified ways to improve the PCII program in order to encourage private sector participation. A full analysis of that program will be forthcoming and will focus on the several issues including the extent to which privately submitted information is disseminated within the government, the risks associated with producing the information, and other business and legal issues surrounding the act.

In addition to PCII, the federal government enacted the Critical Infrastructure Information Act of 2002. The CII Act was passed to provide an exemption from FOIA for private industry critical infrastructure information voluntarily submitted to the federal government. Much like PCII, the CII Act is a good start and the PSP will be analyzing the combined effectiveness of PCII and the CII Act in encouraging the private sector to share CIP information with the government. CII and PCII are just two tools to help the private sector provide needed CIP information to the government and those tools should be strengthened. In addition, PSP will be examining other legal and economic hurdles to information sharing such as Sarbanes-Oxley, liability limitation techniques for information sharing, harmonizing US and international law and making the business case for information sharing and private sector CIP. These topics will be examined in future publications by CIP Program faculty. ❖

Food and Ag Sector *(Cont. from Page 4)* interacts closely with relevant agencies of the federal government. For more information on the support the CIP Program provides to the Food and Agriculture Sector, please see the January 2005 edition of The CIP Report. ❖

[1] GAO Study: http://www.gao.gov /new.items/d05214.pdf

[2] Harvard Report: http://www.hsph.harvard.edu/hcphp/Conference_Proceedings.pdf

Public-Private Cooperation in the Dams Sector

The dams sector is identified as a key resource in HSPD-7 and is considered to be of great importance for homeland security. Dams provide water for drinking, farmland, factories, electricity, recreation, fire suppression, and flood control. In emergencies, dams can store an ample supply of water reserves. According to FEMA, there are now over 10,000 dams in the United States classified as high-hazard potential due to aging and new security concerns resulting from the September 11, 2001 attacks on the United States. The destruction of a dam could have a devastating effect on communities and other infrastructures. The CIP Program has been asked by DHS to facilitate private sector efforts to convene a Dam Sector Coordinating Council to work on securing dams, locks and levees.

Dams in the United States are owned and operated by a mix of public and private entities, including the Federal government. According to the Association for State Dam Safety Officials, about 58% of dams in the country are privately owned, about 16% are owned by local governments, and about 4% are owned by states. The remainder of the dams in the country are owned by the Federal government, public utilities and others. The US Army Corps of Engineers maintains the National Inventory of Dams (NID) and currently has data on 76,000 dams in the United States. A small number of companies own and operate about 30% of dams in the United States. The rest of the dams sector is mostly made up of owner/operators of a small number of dams.

Several government agencies share responsibilities for the safety and security of dams. Under the Interim National Infrastructure Protection Plan, the Department of Homeland Security as the Sector Specific Agency is convening a Government Coordinating Council to bring together government efforts. According to FEMA's National Dam Safety Program, many federal agencies build, own, operate, or regulate dams including the Departments of Agriculture, Defense, Energy, Interior, and Labor, the Federal Energy Regulatory Commission, International Boundary and Water Commission (U.S. Section), Nuclear Regulatory Commission, and the Tennessee Valley Authority. The Federal Energy Regulatory Commission (FERC) licenses large hydropower companies and works very closely with the dams industry on security. The FERC Security Committee with federal and private sector participants works on mitigation and recovery issues to develop guidelines for dam safety. In addition to these federal agencies, the states have a strong role in licensing and working with individual dam owners/operators.

In assisting the sector in its organizing efforts, the Private Sector Program is gathering the names of interested dam owners and operators and will assist in convening an initial organization meeting in Arlington, Virginia. During this first meeting, the non-federal owner/operators of dams will decide on the make up of the council, establish governance for the body, and build the structures for communicating and coordinating with the government on dam safety. ❖

Healthcare *(Cont. from Page 4)*
sectors in the event of any emergency and/or national threat, as well as identifying and addressing risks and interdependencies. The council may also work to raise awareness of the healthcare industry's critical role in the nation's security. Federal partners include the U.S. Departments of Health and Human Services, Department of Homeland Security, Defense, Energy, Interior, Veterans Affairs, Justice, Agriculture, General Services Administration, the Postal Service and the Red Cross.

PSP looks forward to taking on a facilitation role with the National Healthcare and Public Health Sector. Our primary objectives will be to promote efficient communication and awareness among members, and to help construct action plans and provide practical solutions while working with medical facilities, drug manufacturers, suppliers and healthcare providers in an effort to protect the public from terrorist attacks and epidemics. ❖

IT Security and Sarbanes Oxley Compliance

A Roundtable Dialogue of Lessons Learned
Ronald Reagan Building, Washington, DC
Tuesday, May 3, 2005

Since its passage, the Sarbanes-Oxley Act of 2002 (SOX) has engendered spirited debate over the law's implications for corporate information security, especially with respect to the internal control provisions of Section 404. A legal review commissioned by the Cyber Security Industry Alliance (CSIA) concluded that compliance with Section 404 requires publicly traded companies to employ information security to the extent necessary to ensure the effectiveness of internal controls over financial reporting.

In reaching this conclusion, we recognize that, given the size and complexity of IT systems and networks in most publicly traded companies, the statutory and administrative materials governing Section 404 may still lack the detail and specificity regarding IT governance and security that management and auditors might want to guide and inform their compliance efforts. We hope to consider a number of questions in light of collective experiences:

- *Does management and/or the audit community require more detailed and specific guidance on how companies may meet Section 404 compliance requirements for information security?*
- *Should the Public Company Accounting Oversight Board be asked to provide such guidance?*
- *Is additional legal guidance needed or desirable?*
- *If not, how can management and auditors conduct Section 404 activities more efficiently and effectively?*

To address the issues relating to IT security and SOX, CSIA, the Information Systems Security Association, the Information Systems Audit and Control Association, and George Mason University's CIP Program are hosting a daylong roundtable discussion of lessons learned from SOX compliance. The event will feature four separate panels covering: 1.) corporate and financial management; 2.) internal and external audit; 3.) corporate and outside counsel; and, 4.) information security professionals.

To register for this event, please go to: http://pfidc.com/sox/index.htm. There is a $95 registration fee for all attendees.

Water Sector *(Cont. from Page 5)* mechanism, which will be available to all sectors. The Homeland Security Information Network (HSIN) is in a pilot test for the water sector and the WSCC information sharing task group is looking at the pilot test and the WaterISAC to evaluate how the two could work together in furthering the sector's information sharing goals, which includes a broad reach for disseminating threat information to all water and wastewater related utilities.

The sector has very robust research and development programs. The Water Environment Research Foundation and AWWA Research Foundation both have full programs for security related research. The foundations are working with the Council to map out existing research including Federal government efforts and to determine if any gaps in research exist. This group also represented the sector at a cross sector R & D Workshop.

In addition to these issues, the Water Sector Coordinating Council will be instrumental in further implementing the Interim National Infrastructure Protection Plan, incorporating the owner/operator perspective, and then incorporating it across the nation to secure water and wastewater systems. The main purpose for convening broad representation of the water sector is to provide an opportunity for private, public, urban, and rural systems to provide strategic input to the national plans for protecting the nation's water systems and the people who rely upon them. ❖

Cyber Security and the Law: Addressing Compliance, Complexity, and Confusion

The Cyber Security Industry Alliance and The Critical Infrastructure Protection Program at George Mason University School of Law present a three-part symposium on the emerging landscape of cyber security legislation and compliance. The frequency and complexity of legislation surrounding cyber security has exploded in the past two years. As our lives and commerce become increasingly dependent on IT systems, the interaction of existing laws and proposed legislation becomes more and more complex. This symposium series explores the complex emerging framework of multi-level legal and technology compliance requirements.

SAVE THE DATES:

April 26 (Federal Level) May 26 (International Level)

The April 26 event will be held at 6:15 p.m. at 2099 Pennsylvania Ave., Holland and Knight, Suite 100, Washington D.C.; the final session of this three-part series will be held May 26 near Capitol Hill. A keynote speaker or panel will focus on a specific legislative and compliance arena each evening, with a wine and cheese reception and discussion to follow.

Federal-Level Cyber Security Compliance
Tuesday, April 26 (Washington, D.C.)
6:15-8:00 pm

Sarbanes Oxley, HIPAA, and the Telecommunications Act of 1996 were all originally passed to deal with non-cyber security issues - yet each affects how data is transmitted, processed and compiled. The development of case law interpreting these statutes is also likely to determine how broadly federal law impacts cyber security. This session explores the federal landscape and the potential trajectory of judicial interpretation.

Invited speakers include...

- Jessica Herrera, Chief Counsel and Deputy Staff Director to the House Committee on Homeland Security, Democratic Office.
- Steve DeVine, Chief Counsel and Deputy Staff Director to the House Committee on Homeland Security, Republican Office.
- Mike Sozan, staff of Sen. Nelson D-FL
- Frank Cavaliere, staff of Sen. Allen R-VA
- Rod Nydam, Associate Director in charge of Private Sector Programs of the GMU CIP Program
- Paul Kurtz (Moderator), Former Special Assistant to the President, Executive Director, Cyber Security Industry Alliance

Space is limited
RSVP now to Amy Cobb, 703-993-8193 or acobb1@gmu.edu
CLE credit may be available.

YOU ARE CORDIALLY INVITED...

For the Fourth in a Series of Critical Conversations on Infrastructure Protection
Sponsored by
The Critical Infrastructure Protection Program (CIP Program),
Part of The George Mason University School of Law

Getting Serious About Cyber Security

Wednesday, May 18, 2005
Lunch: Noon
Newsmaker Panel Discussion: 12:30 - 2 p.m.

The National Press Club
The Holeman Lounge
529 14th Street, N.W.
Washington, D.C.

R.S.V.P. (703) 993-4722
Please note that this is a free event and seating is limited.

Panelists to Include:

Tom Davis *(R-VA), Chairman*
Committee on Government Reform

Rep. Zoe Lofgren *(D-CA), Ranking Member*
House Subcommittee on Cybersecurity, Science, and Research & Development

Paul Kurtz*, Former Special Assistant to the President*
Executive Director, Cyber Security Industry Alliance

Pamela Fusco*, Chief Security Officer, Merck & Co., Inc.*

Marian Hopkins, *Director, Public Policy, Business Roundtable*

Moderated by Frank Sesno
Senior Fellow, Critical Infrastructure Protection Program

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.