THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 7 NUMBER 1

JULY 2008

CONFERENCE SUMMARIES

EDITORIAL STAFF

EDITORS
Morgan Allen
Elizabeth Jackson
Olivia Pacheco

STAFF WRITERS
Tim Clancy
Maeve Dion

JMU COORDINATORS
Ken Newbold
John Noftsinger

PUBLISHING
Zeichner Risk Analytics
Contact: CIPP02@gmu.edu
703.993.4840

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

Featured in this month's issue of *The CIP Report* is information on conferences hosted by the CIP Program at George Mason University and its partner, James Madison University (JMU), as well as CIP Program participation in a Worldwide Business Research event focused on the Energy Sector. Coinciding with the conference subject-matter is also the concept of public-private partnerships.

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

The Institute for Infrastructure and Information Assurance (IIIA) at JMU co-hosted, along with the Federal Facilities Council of The National Academies, the 2008 Homeland Security Symposium, *Fostering Public-Private Partnerships*, on May 22nd. Articles authored by IIIA present an event overview and summary of symposium proceedings, including excerpts from the day's keynote speeches.

From May 13-15th, the CIP Program co-hosted the Security Analysis and Risk Management Association's (SARMA) 2nd National Conference on Security Analysis and Risk Management. This issue provides a conference overview and articles on select topics addressed at the conference, including a contribution from the U.S. Government Accountability Office (GAO) on its Forum on Strengthening the Use of Risk Management Principles in Homeland Security and pieces capturing information on presentations on business cases for enterprise risk management (ERM), various government approaches to risk management and assessment, safeguarding supply chains, and cyber security. An overview of SARMA and current projects underway is also offered.

Recognizing the CIP Program's research on Energy Sector issues, its staff were invited to present on cyber security issues with respect to the smart electric grid and participate in a panel on public-private coordination at Utilities Field Service 2008. This operations strategy and asset management event, held from May 28-30th, focused on topics such as data integration, response and reliability, and more. This month's *Legal Insights* discusses public-private partnerships and the shared responsibility they entail. Also included in this issue is an announcement of the release of a paper co-authored by one of the Program's legal researchers for the Organisation for Economic Co-operation and Development (OECD).

Finally, it is with great pleasure that we announce the appointment of the CIP Program's new director, Mick Kicklighter. A copy of the press release naming Kicklighter as the new director is found on page 18. We hope you enjoy this issue and the summaries provided of recent events dedicated to exploring key homeland security topics, and appreciate your continued support as we welcome Mick Kicklighter to the CIP Program team.

2008 Homeland Security Symposium *Conference Overview*

by Dr. John B. Noftsinger, Jr.,
Vice Provost for Research and Public Service and Executive Director, JMU IIIA

The Institute for Infrastructure and Information Assurance (IIIA) at James Madison University (JMU) in partnership with the Federal Facilities Council of The National Academies was pleased to host the 2008 Homeland Security Symposium, *Fostering Public-Private Partnerships*, on May 22nd at the National Academy of Sciences in Washington, D.C. This was the third symposium sponsored by JMU and the Federal Facilities Council which brought together leaders from government, the private sector, and academe to discuss timely issues and explore solutions to problems within homeland security. The focus of this year's symposium was on the topic of public-private partnerships. As the complexity within critical infrastructures increases the relationship between government and industry, public-private partnerships become even more essential to advance the efforts to secure our homeland. Well-coordinated partnerships between industry and government bring the full capabilities of industry squarely into the national preparedness and response agendas. The primary goal of this symposium was to advance the dialogue on the importance of collaboration by providing examples of successful partnerships across the levels of government (federal, state, and local). The models presented at the symposium highlighted how preparedness and response efforts are more effective when organizations work together towards a common goal.

Symposium participants included leaders from academe, federal/state/local government agencies, private sector companies, industry associations, and standards organizations. Rep. Dutch Ruppersberger (MD-2) and Al Martinez-Fonts, Assistant Secretary for the Private Sector Office, U.S. Department of Homeland Security (DHS), provided insightful keynote addresses to complement the panel presentations. This unique cross-section of participants presented an opportunity to learn from existing partnership models and perhaps, more importantly, develop new collaborative relationships. For further information on the symposium or to request proceedings, please visit: www.jmu.edu/iiia/2008symposium/index.html. ❖

Congressman Dutch Ruppersberger (MD-2) addressing the audience

DHS Assistant Secretary for the Private Sector Office Alfonso Martinez-Fonts speaking to participants

Summary of the Proceedings of the 2008 Homeland Security Symposium *Fostering Public-Private Partnerships*

by Dr. George H. Baker, Associate Director for Infrastructure Assurance, and
Cheryl J. Elliott, Assistant Director for Marketing and External Relations, JMU IIIA

The theme of the third annual JMU IIIA Homeland Security Symposium, *Fostering Public-Private Partnerships*, was based on an important conclusion from our 2007 symposium, *Cascading Infrastructure Failure: Avoidance and Response*. Recent U.S. high-consequence events have clarified the importance of government collaboration with industry. The benefit of such collaboration was one of the most important lessons learned from Hurricane Katrina. The resources owned and controlled by American industry dwarf those available to local, state, and even federal government departments. Better agreements and incentives to bring the full capabilities of industry squarely into the national response agenda will be indispensable in effectively responding to large-scale catastrophes. At our 2007 symposium, General Russel Honoré, who led the National Guard response to Katrina stated, "We need the partnering between local, state, and federal governments; but the biggest partner should be industry . . . because people in industry, if they understand the problems, can take them on as business opportunities."

The 2008 event program was structured to illuminate exemplary public-private partnerships at the local, regional, and national levels and consider steps to develop and improve public-private partnerships for the future. The program included presentations by recognized experts from government and industry engaged in operating and securing critical infrastructures. Participants represented academe, federal/state/local government agencies, private sector companies, industry associations, and standards organizations.

Morning Keynote

Congressman C.A. "Dutch" Ruppersberger, Maryland 2nd District, serves on the Appropriations Committee; the Technical and Tactical Intelligence Subcommittee; the Terrorism, Human Intelligence, Analysis, and Counterintelligence Subcommittee; and the Oversight and Investigations Subcommittee.

Congressman Dutch Ruppersberger (MD-2) emphasized the importance of government-industry partnerships, but also stressed the importance of academe in solving homeland security problems. His district relies heavily on expertise from Johns Hopkins University, the University of Maryland, and Towson University. His talk focused on two technical areas in need of improved public-private partnerships: intelligence satellites and cyber security. In these areas, two domains come into play — real space and virtual space. With respect to intelligence satellites, the government owns the satellite hardware and defines the projects and parameters. Yet, most of the work associated with satellite development is done through the private sector. Cyber security is an area where the government has only limited control because the networks and enterprises are mostly privately owned and controlled. Both areas require strong partnerships between government, industry, and academe if our national security is to be ensured.

Speech Excerpt:

A major source of U.S. strength is our ability to control the skies. Our ability to control the skies is being challenged by other nations, notably Russia and China. To maintain our capabilities, we need to build the next generation of satellites quickly. Private sector involvement with its best practices and expertise is critical for success.

Development timelines and costs of satellites are increasing. After Sputnik, President Kennedy challenged the technical community to achieve a moon landing. NASA seized the initiative and achieved this objective in twelve years. At present, we have difficulty developing and deploying a satellite in twelve years. It is clear we need to put a higher premium on R&D in the U.S. Intelligence

(Continued on Page 4)

JMU Symposium *(Cont. from 3)*

satellite shortfalls are worrisome given the challenges posed by Russia and China.

Many of the problems are a result of the lack of communication between government and industry. Contractors are not asked the right questions in the Request for Information (RFI) processes. Contractors are not clear on requirements. The government often rushes to get RFIs out against arbitrary deadlines. It is often assumed that uncertainties, specifications and unknown factors inherent in RFIs can be fixed by future renegotiation; however, we need to plan for unknowns up front.

Satellite procurement problems are easy to solve compared to cyber security. In the case of satellites, the government can specify performance requirements. Since the government does not control Internet, it is very difficult to secure, especially so, considering everything connected to it. Ninety-eight percent of Internet traffic runs on private networks. The Internet is "owned by everyone . . . controlled by no one."

A major objective with respect to cyber security is protecting the banking sector. Bank networks are continuously under attack. A major successful attack would result in an unprecedented bank run. Financial markets would panic. Even if the network were only down for a day there would be catastrophic consequences for our economy.

A network is only secure as its weakest point. Our national security networks are connected to the outside world. The ability to disrupt our networks has fundamentally altered the strategic landscape. Public-private partnerships are essential to secure every network in the U.S. because the government cannot decide how to organize and secure the Internet and then hire someone to do it. Every company with a server in its back room needs to be involved with this effort. Universities play a major role in growing our network security workforce.

PANEL 1 – Local Public-Private Partnership: Nassau County, New York's Security/Police Information Network

Panelists: *Assistant Chief Paul Tully, Nassau County Police Department, Moderator; Detective Sergeant William Leahy, SPIN Coordinator, Homeland Security and Counter Terrorism Bureau, Nassau County Police Department; Oksana Farber, insurance industry professional; and Mario Doyle, Director of the Police Reserve Force for Nassau County.*

The Security/Police Information Network (SPIN) is a dynamic, multi-dimensional crime prevention partnership including Nassau County Police Department, the public, and business. It connects federal, state, and local government agencies with transportation and other infrastructure services. It is essentially a virtual public-private partnership (VP3) that seeks to increase public safety through the sharing of important and timely information.

The network is organized into concentric rings. Federal/state/local law enforcement is in the center. Government is the second ring. Critical infrastructure service providers and individual businesses are the third, outer ring. Created by the Nassau County Police Department in 2004, SPIN utilizes e-mail coupled with live meetings to provide private sector partners with the information they need to protect themselves, their families, their communities, and their organizations. In addition, the VP3 has enabled the Police Department to leverage the private sector in order to prevent crime, arrest offenders, and otherwise maintain safer communities.

Taking an "all-crimes, all-threats, all-hazards" approach to information sharing, SPIN supports wide-ranging missions — from homeland security and business continuity to crime prevention and emergency preparedness. This broad approach is not only advantageous to private sector partners, but facilitates intergovernmental partnerships, as the need for information has brought about collaboration between the Police Department and the Office of Emergency Management, Department of Health, the Fire Commission, and the local public transportation agency. The network has grown exponentially from 175 security directors at its inception to more than 800 security directors from nearly every sector and critical infrastructure, 125 business and community leaders, 100 government employees, and over 300 members of federal, state, and local law enforcement.

(Continued on Page 19)

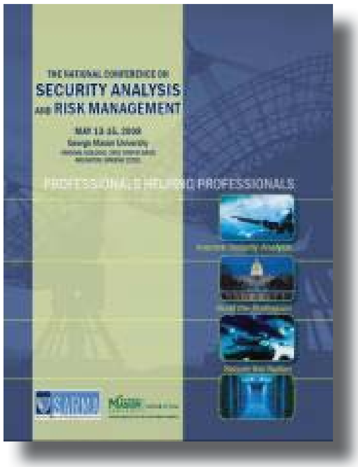
2nd National Conference on Security Analysis and Risk Management *Conference Overview*

The CIP Program co-hosted the Security Analysis and Risk Management Association's (SARMA) 2nd National Conference on Security Analysis and Risk Management, held on the George Mason University Arlington Campus from May 13-15, 2008. The conference featured six keynote and plenary session speakers, 35 technical sessions with over 40 speakers, and 10 exhibitors. Approximately 200 individuals participated in the conference and garnered a wealth of information on current efforts with respect to risk management in both the public and private sectors, in the United States and abroad.

As stated by SARMA, the intent of the conference was to bring together "leaders, experts and practitioners in security analysis and risk management to share current developments and evolving best practices in the protection of the nation, its people, critical infrastructures, information and operations from terrorism and other man-made and natural hazards." As also relayed by SARMA, highlights of the conference included:

- National policy-makers addressing the future of security risk analysis policy
- Experts on analysis of terrorist, counterintelligence, criminal, and other threats
- Well-known practitioners from DHS, U.S. Department of Defense (DoD), Transportation Security Administration (TSA), U.S. Coast Guard (USCG), and other civil agencies
- Recent advances and research in security risk management techniques
- Recent contributions to the professional body of knowledge in security analysis
- Practitioners discussing common issues and real-world solutions to today's needs

The topics of conference presentations ranged from various government approaches to risk management and risk assessment to modeling and simulation analysis to business cases for risk management, and more. Select topics are addressed through articles in this issue of *The CIP Report*. Additional topics will be featured in SARMA's newsletter, *The Risk Communicator*, and on its website. The March-May 2008 issue of *The Risk Communicator* also offers valuable insight on the conference proceedings from SARMA leadership.



Notably, the conference afforded participants the opportunity to interact with government representatives directly responsible for carrying out risk-related initiatives on the federal, state, and regional levels. It also allowed for the exchange of ideas, best practices, and lessons learned with representatives of the private sector, including non-profit organizations and academic institutions. Moreover, the conference featured a presenter from Australia, who informed participants of the strides his country is making with respect to risk management standards, and a presenter from the European Union (EU), who offered insight on information sharing efforts underway in the EU and how they feed into the better management of threats and vulnerabilities. The experiences of these two presenters spurred much discussion, particularly on how the United States could leverage their work to improve its own efforts to enhance security and mitigate risks posed to the U.S. population, economy, and infrastructure.

Overall, the conference proved an excellent forum for exploring current and envisioned security analysis and risk management practices. The CIP Program was exceedingly pleased to co-host this valuable conference and further develop its partnership with SARMA.

For more information on the conference, please visit http://cipp.gmu.edu/research/SARMAconference.php or http://sarma.org/events/past events/2ndnationalconfere/. Information on SARMA and its many initiatives can be found at http://www.sarma.org. ❖

(Continued on Page 6)

SARMA Conference *(Cont. from 5)*

Speaker Organizations

Government

- Homeland Security Council
- Interagency OPSEC Support Staff
- National Defense University *
- New York State Office of Homeland Security
- U.S. Department of Defense
    - Defense Threat Reduction Agency
    - Office of the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs)
    - U.S. Army
- U.S. Department of Homeland Security
    - Federal Emergency Management Agency, Office of National Capital Region Coordination
    - Federal Protective Service
    - Homeland Infrastructure Threat and Risk Analysis Center
    - Office of Infrastructure Protection
    - Science and Technology Directorate
    - Transportation Security Administration
    - U.S. Coast Guard
- U.S. Department of the Interior, Bureau of Reclamation
- U.S. Government Accountability Office

Non-Government

- AcuTech Consulting Group
- Alion Science and Technology
- Applied Research Associates, Inc.
- CENTRA Technology, Inc.
- Centurion Holdings, LLC
- Cybrinth, a duostech company
- George Mason University
- Georgetown University
- Good Harbor Consulting, LLC
- Innovative Decisions, Inc.
- Jakeman Business Solutions Pty Ltd / Risk Management Institution of Australasia
- MITRE Corporation
- Pacific Disaster Center
- Pennsylvania State University
- Perigean Technologies LLC
- RAND Corporation
- Teledyne Brown Engineering
- The Tauri Group
- Symantec Corporation (Europe, Middle East and Africa Strategic Team)
- University of Virginia

** NDU is an accredited graduate-level university that operates under the direction of the Chairman of the Joint Chiefs of Staff*

Conference Exhibitors

- Security Analysis and Risk Management Association
- George Mason University School of Law, Critical Infrastructure Protection Program
- Alion Science and Technology
- Applied Research Associates, Inc.
- Booz Allen Hamilton
- Interagency OPSEC Support Staff
- National Defense Industrial Association
- PricewaterhouseCoopers
- SRA International, Inc.
- U.S. Department of Homeland Security (National Infrastructure Protection Plan Program Management Office)

Conference Sponsors

PRICEWATERHOUSECOOPERS

SRA INTERNATIONAL, INC.

Booz | Allen | Hamilton

CYBRINTH a duostech company

GAO Forum on Strengthening the Use of Risk Management Principles in Homeland Security

by the Homeland Security and Justice Team, U.S. Government Accountability Office

From the terrorist attacks of September 11, 2001, to the tragic events of Hurricane Katrina, homeland security risks vary widely. Many have pointed out, as did the Gilmore and 9/11 Commissions, that the nation can neither achieve total security nor afford to protect everything against all risks. Managing these risks is especially difficult in today's environment of globalization, increasing security interdependence, and growing fiscal challenges for the federal government. It is increasingly important that organizations effectively target homeland security funding — totaling nearly $65 billion in 2008 federal spending alone — to address the nation's most critical risk priorities. To assist both Congress and federal agencies, including DHS, the Government Accountability Office (GAO) convened a forum to advance a national dialogue on applying risk management to homeland security.

On May 14, 2008, GAO Director Cathy Berrick presented the results of this forum at the 2nd National Conference on Security Analysis and Risk Management. Ms. Berrick is a senior executive with GAO's Homeland Security and Justice Team, where she oversees reviews of aviation and surface transportation security matters and DHS management issues. This article will share the highlights of Ms. Berrick's presentation.

Recognizing that risk management helps policymakers make informed decisions, Congress and the administration have charged federal agencies to use a risk-based approach to prioritize resource investments. Nevertheless, federal agencies often lack comprehensive risk management strategies that are well integrated with program, budget, and investment decisions. To provide a basis for analyzing these strategies, GAO has developed a risk management framework based on industry best practices and other criteria. This framework, shown in Figure 1, divides risk management into five major phases: (1) setting strategic goals and objectives, and determining constraints; (2) assessing risks; (3) evaluating alternatives for addressing these risks; (4) selecting the appropriate alternatives; and (5) implementing the alternatives, and monitoring the progress made and results achieved.

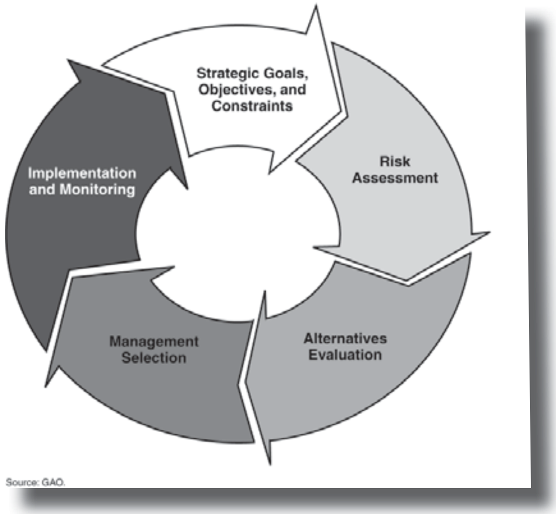

Strategic Goals, Objectives, and Constraints
Risk Assessment
Alternatives Evaluation
Management Selection
Implementation and Monitoring
Source: GAO.

Figure 1: GAO Risk Management Framework

On October 25, 2007, the Comptroller General convened a diverse array of experts from the public and private sectors, including, from the public sector, a former governor, a former DHS under secretary, a U.S. Coast Guard Admiral, and senior executives from DHS, the U.S. Army, and the National Intelligence Council, as well as state and local officials with homeland security responsibilities. From the private sector, participants included executives from leading multinational corporations such as Swiss Re, Westfield Group, JPMorgan Chase, and Wal-Mart. In addition, several of the world's leading scholars from major universities, the National Research Council, and the RAND Corporation participated in the forum. GAO asked the forum participants to identify: (1) effective risk management practices used by organizations from the public and private sectors, and (2) key challenges faced by public and private organizations in applying risk management principles to homeland security and actions that could be taken to address these challenges.

Forum participants began by identifying what they considered to be effective public and private sector risk management practices. For example, participants discussed

(Continued on Page 8)

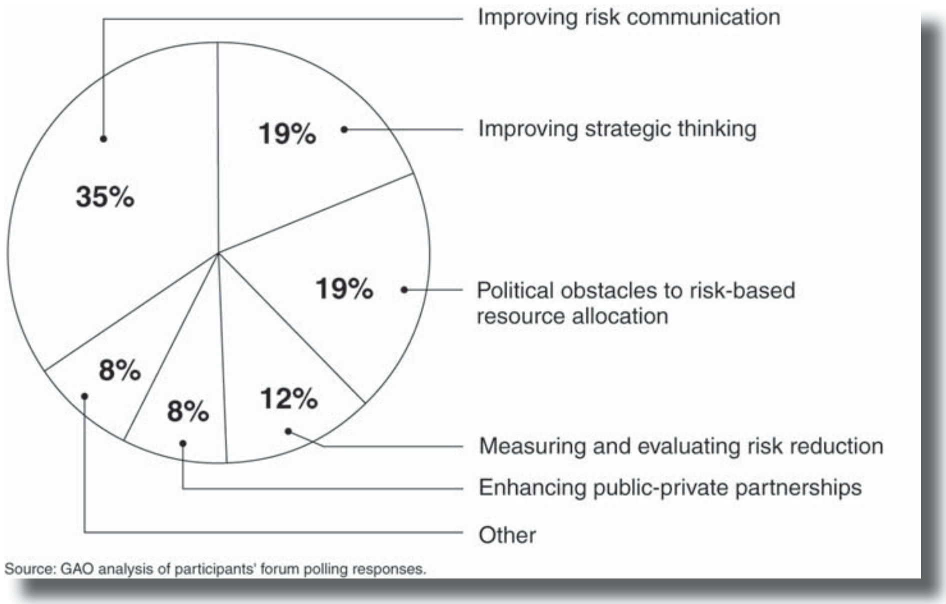
GAO Forum *(Cont. from 7)*

the private sector use of a chief risk officer, though they did not reach consensus on how to apply the concept of the chief risk officer to the public sector. One key practice for creating an effective chief risk officer, participants said, was defining reporting relationships within the organization in a way that provides sufficient authority and autonomy for a chief risk officer to report to the highest levels of the organization. Participants stated that the U.S. government needs a single risk manager. One participant suggested that this lack of central leadership has resulted in distributed responsibility for risk management within the administration and Congress and has contributed to a lack of coordination on spending decisions. Participants also discussed examples of public sector organizations that have effectively integrated risk management practices into their operations, such as the U.S. Coast Guard, and compared and contrasted public- and private-sector risk management practices.

According to the participants at GAO's forum, three key challenges exist to applying risk management to homeland security: improving risk communication, political obstacles to allocating resources based on a consideration of risk, and a lack of strategic thinking about managing homeland security risks. Many participants, 35 percent, agreed that improving risk communication posed the single greatest challenge to using risk management principles (see Figure 2). Further, 19 percent of participants stated political obstacles to risk-based resource allocation were the single most critical challenge, and the same number of participants, 19 percent, said the single most critical challenge was a lack of strategic thinking. The remaining participants identified other key challenges, for example, technical issues such as the difficult but necessary task of analyzing threat, vulnerability, and consequences of a terrorist attack in order to assess risk; partnership and coordination challenges; and the need for risk management education.

The expert panel also identified ways to address some of these challenges. To better communicate about risks, participants recommended that we educate the public and policymakers about the risks we face and the value of using risk management to establish priorities and allocate resources; engage in a national discussion to reach a public consensus on an acceptable level of risk; and develop new communication practices and systems to alert the public during an emergency. To better allocate resources based on risk, participants recommended that public officials and organizations consider investing in protective measures that yield long-term benefits. In addition, to address strategic thinking challenges, participants recommended the government develop a national strategic planning process for homeland security and government-wide risk management guidance. To improve public-private sector coordination, forum participants recommended that the private sector be more involved in the public sector's efforts to assess risks and that more state and local practitioners and experts be involved through intergovernmental partnerships.

For additional details on GAO's Forum on Strengthening the Use of Risk Management Principles in Homeland Security, we encourage you to read the full report, GAO-08-627SP, at http://www.gao.gov/new.items/d08627sp.pdf. For more information, contact Cathy Berrick at (202) 512-8777 or berrickc@gao.gov. ❖



Source: GAO analysis of participants' forum polling responses.

Figure 2: Key Challenges in Applying Risk Management to Homeland Security

Risk Management for Private Sector Enterprises

by James Creel, Project Associate

As seen by the September 11th attacks and Hurricane Katrina, enterprise risk management (ERM) has emerged as a central component of business operations and continuity. While companies invest many resources to enhance profits and financial growth, preparation and mitigation failures in the event of an emergency can have severe consequences. Financial outlooks for companies can be dim if they do not make concerted efforts to protect critical infrastructure and key resources (CI/KR).

DHS is establishing frameworks within the public and private sectors to address risk management and risk-based approaches to critical infrastructure protection through the National Infrastructure Protection Plan (NIPP). The primary objective of the NIPP is to "[b]uild a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR . . . and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency."

This is a difficult challenge for DHS as approximately 85% of U.S. CI/KR are owned and operated by the private sector. Motivating the private sector in regards to its risk management protocols is of the utmost importance. There is, however, a fine line between engaging the private sector and regulating it. Both public and private partners hope to avoid federal regulation in private industry. Yet, there is an inherent lack of transparency into vulnerability and risk mitigation within the private sector. It is difficult to determine whether risk management procedures in the private sector are meeting the standards set forth in the NIPP.

Although ERM has increased in prominence in recent years, it is not a new concept. Demonstrating the importance of ERM, it was a key theme discussed at the 2nd National Conference on Security Analysis and Risk Management co-hosted by George Mason University and SARMA.

Security has become an intangible asset for companies according to Robert Liscouski, President, Advisory and Forecasting, and a partner in Centurion Holdings, LLC. Proper management of security procedures can lead to higher earnings by reducing vulnerabilities. It is clearly in companies' short- and long-term interests to maintain such risk protocols.

Liscouski asserted that security is vital in preventing future adverse effects on a company and its shareholders. Creating stable corporate environments through risk mitigation and resilience afford both physical and emotional benefits. Recognition of security as an intangible asset, however, must become a corporate priority. Resilience and sustainability from a security perspective are as critical to corporate interests as profits.

Companies must identify their security priorities first and foremost, e.g., cyber risks, physical risks, and insider threats from personnel. Managing these risks in an uncertain threat environment will continue to pose challenges for CEOs. Security is a priority and this must be a resolute concept. Companies must be willing to make the commitment and avoid complacent or apathetic attitudes regarding security and risk. This will take investment of corporate resources, as well as dedication to determining the "right" level of security for each company given the predicted return on investment.

Julian Talbot, Director of the Risk Management Institution of Australasia and Senior Consultant with Jakeman Business Solutions, also spoke at the conference on the topic of business cases for risk management. Talbot reiterated the need for risk-informed decision-making to improve security risk management (SRM) within enterprises. A valuable component of this is the development of structured cost-benefit methods to assess appropriate measures to mitigate risk commensurate with an enterprise's business model.

Like Liscouski, Talbot asserted that operating priorities must be established early in the SRM process.

(Continued on Page 24)

Approaches to Risk Management and Assessment

Risk management and assessment are important components within the private and public sectors. Both have set up their own approaches and different methodologies to establish security measures within their organizations. The following are some examples of the different approaches taken directly from information presented at the recent SARMA conference.

Federal Protective Service

The Risk Assessment and Management Program (RAMP) is a new assessment tool being developed. It will provide a single source for the collection, storage, and analysis of building information. RAMP will be used to:

- Assess and analyze risks posed to Federal facilities from crime, natural hazards, and terrorism
- Centrally store, access, and report risk assessment findings
- Manage all aspects of the Building Security Assessment process
- Recommend and track the implementation of countermeasures throughout their lifecycle
- Perform inventory-wide analysis of the risks posed to Federal facilities and the means of reducing them

RAMP will be implemented in three phases. The first phase will include all basic functionality necessary to conduct and report on risk management for federal facilities. The second phase will provide enhanced information sharing and reporting capabilities. Finally, the third phase will include additional functionality and will be fully capable of being rolled out to security partners.

New York State

Critical Infrastructure Suspicious Activity Reporting (CISAR) is a new tool for intelligence analysts that combines suspicious activity reporting, infrastructure data and statewide datasets in one system for geospatial analysis. It will assist the state in supporting a full range of intelligence cycle activities. CISAR's capabilities include:

- Threat/Vulnerability Overlays
- Allows for the identification and analysis of patterns of suspicious behavior
- Data Analysis
- Visualization/Mapping

Project participants include: New York State Office of Homeland Security, New York State Police, New York State Office of Cyber Security and Critical Infrastructure Coordination, and New York State Intelligence Center.

DHS, Science and Technology Directorate

DHS's efforts are working towards a more comprehensive and better integrated collective approach to risk-informed decision-making. This process is described through the Risk Management Cycle. It begins with 1) Identify Potential Risk, 2) Assess Potential Risk, 3) Develop Action Plan, 4) Implement Action Plan, and 5) Measure Impact and Cost. There are three different decision types within the DHS Risk-Informed Decision Matrix. They include Strategic, Operational, and Tactical. Risk analysis considers the following:

- Threat
- Vulnerability
- Consequences
- Projected Impact/Benefit of Alternative Courses of Action
- Benefit/Cost Analysis
- Identify decision-irrelevant variables and factors
- Eliminate clearly inferior options
- Focus on what can be done, not what to worry about

U.S. Department of Defense

Defense Critical Infrastructure (DCI) will be protected through a risk management approach that supports the prioritization of scarce resources, while focusing priorities on assets at greatest risk, based on assessed criticality, vulnerability, and threats and hazards. Risk assessment identifies critical assets, threats and hazards, and vulnerabilities. Risk response includes:

- Accept Risk
- Mitigate the Threat/Hazard
- Remediate the Risk
- Reconstitute Lost Capability

U.S Coast Guard

The Maritime Security Risk Analysis Model (MSRAM) was designed to enhance security and reduce the risk of terrorism by identifying and prioritizing critical infrastructure, key resources and high consequence transits and events across sectors

(Continued on Page 24)

Ties That Bind: Safeguarding Supply Chains in a Global Economy

by Joseph Maltby, Law Intern

The genius of the global economy is how the interests of vast numbers of people are aligned in such a way as to make an almost inconceivably complex system seem simple. The steps that bring even simple commodities to your door are too numerous to mention and each individual act is dependent on hundreds of other actors doing their part, without even knowing the ultimate purpose of their actions. This global system is an efficient method of delivering goods and services and allows for a standard of living that would be the envy of the most decadent Roman emperor (notwithstanding the lack of gladiators).

Yet, this same complexity is cause for alarm when we live in a world with so many different ways to bring the system crashing down. Guarding against these threats to the global supply chain is the subject of a presentation by Professor Celina Realuyo at the SARMA conference. Professor Realuyo educates top U.S. and foreign military and civilian leaders on national security and counterterrorism strategies at the National Defense University, teaching the "Global War on Terrorism" and "Terrorism and Crime" courses.

The same soil that has nourished our global economy has also birthed truly global threats to our livelihoods, our health, and even our lives. Terrorism, international crime, pandemics, climate change, the competition for natural resources (even those once considered limitless, like water), war, and systemic technological failures. These are the dark shadows lurking in the corners of the dream of prosperity and peace that animates our endeavors. A global economy makes it possible to arrange criminal enterprises that span continents, or to create a terror network to strike the most powerful country in the world from a mountain cave, or to allow a disease picked up in India to infect travelers from China to the United States to France in the span of a week.

Supply chains represent a concrete example of our vulnerability. Imagine the effect of severing even a few of the links of the chain. The recent tomato crisis is a perfect example of how disruptions that were once local have been "let out of the box" by the global economy in something akin to a mutated version of the butterfly effect. And this was an accidental event. If it is that easy to disrupt the economy through negligence, how easy would it be to deny access to dozens of products with a few well-targeted attacks?

Now, a counterargument to this theory is the point that the same complexity that makes the system vulnerable will also prove to be its source of resilience. When one supply chain is disrupted, it is relatively easy to find an alternative and the economy keeps humming. This is true in most situations, oil being one dramatic exception, but business managers want more than just the knowledge that their businesses will stay open. They want a method for minimizing their risk and profit loss from these events.

To truly manage this risk requires an investment in enterprise risk management. Corporations are already accustomed to dealing with the risks carried by the credit market or from operating within

(Continued on Page 23)

Upcoming Supply Chain Event

The CIP Program will co-host an event on Supply Chain Security, Resilience & Sustainability on Friday, October 17, 2008. This one-day conference will be held on the George Mason University Arlington, Virginia Campus.

For information on the event, including a "Save the Date" announcement that features the names of all event hosts, please visit http://cipp.gmu.edu/research/SupplyChainConference.php. This webpage will be updated regularly as additional information becomes available.

Cyber Presentations at the SARMA Conference

Many discussions at the recent conference included issues relating to technology, and four of the speakers had a specific cyber focus. Paul Kurtz, Stephen Spoonamore, Arun Sood, and Irv Lachow presented on various aspects of the interplay of technology and security analysis and risk management.

Paul Kurtz

Cyber Warfare and Governments' Awakening

Paul Kurtz opened with an overview of events over the past year that led to an awakening among key governments to the risks of poor information security. He discussed the implications of greater government attention to this issue for the information, communications, and telecommunications industries, as well as the defense industrial base. Kurtz's comments evolved from his experience as a recognized cyber security and homeland security expert, having served in senior positions on the White House's National Security Council (NSC) and Homeland Security Council under Presidents Clinton and Bush; as a member of the President's Commission on Critical Infrastructure Protection, where he developed the international component of the *National Strategy to Secure Cyberspace*; as a director for counterterrorism in the NSC's Office of Transnational Threats; and as the founding Executive Director of the Cyber Security Industry Alliance (CSIA), an advocacy group dedicated to ensuring the privacy, reliability, and integrity of information systems through public policy, technology, education, and awareness. Kurtz is currently a partner and COO of Good Harbor Consulting, LLC.

Stephen Spoonamore

A Capability Maturity Model Approach to SCADA Risk Analysis

A variety of risk analysis methods that were developed for information technology, business, and economic applications have been applied to Supervisory Control and Data Acquisition (SCADA) and related industrial control systems. However, as Stephen Spoonamore discussed in his presentation, SCADA systems have unique characteristics and requirements that have to be considered and addressed in conducting risk analyses. For example, programmable logic controllers (PLCs) on Ethernet networks can malfunction when exposed to scanning Internet Control Message Protocol (ICMP) messages. Because of the complexity and real-time nature of control systems, they are also increasingly vulnerable to hardware failures and administrative security faults, such as running unauthorized software on plant floor computers. Local control elements in a plant have memory and processing limitations and cannot accommodate suites of security-related software without affecting plant performance and safety. These limitations sometimes preclude the implementation of authentication or encryption. In the world of industrial control, plant operations, product quality, production, and safety trump information system security. Because of real and imagined concerns, disabling unnecessary software capabilities or applying patches is not performed as required.

In his presentation, Spoonamore proposed a Capability Maturity Model (CMM)–based risk analysis process that considers the continuous improvement paradigm. The CMM supports continuous reduction of residual risk by focusing on the unique real-time and near real-time characteristics and operational requirements of SCADA and industrial control systems. The associated risks are specified in Base Practices that are grouped into key Process Areas (PAs). The PAs of the CMM will embody the innate characteristics of SCADA and control systems in analyzing risk and not affect a sometimes force-fit of IT risk analysis methods to entities comprising the nation's critical infrastructure. Spoonamore's presentation can be found on SARMA's conference webpage.

In developing his risk analysis process, Spoonamore drew on his past cyber security work for various government agencies and elements of the United States Armed Forces. In his current role as founder and CEO of Cybrinth, Inc., Spoonamore developed methodologies and best practices that have become standards in the credit

(Continued on Page 13)

Cyber Presentations *(Cont. from 12)*

card industry. Spoonamore has also contributed to standards development for E-Authentication of Identity and the EPAD All-Hazards National Alert System.

Arun Sood

Self Cleansing Intrusion Tolerance – A Proactive Risk Management Strategy

As Arun Sood emphasized in his presentation, the complexity of modern information services, and the sophistication, pace, and variety of attack techniques, requires a new thinking about the computer security problem. In spite of large investments in computer security, attackers continue to evade the most advanced intrusion prevention and detection systems. According to Sood, the problem stems in large part from the constant innovation and evolution of attack techniques, and rapid development of exploits based on recently discovered software vulnerabilities. The sophisticated cyber attacks lend importance to the concept of intrusion tolerance: a critical system must fend off, or at least limit, the damage caused by unknown and/or undetected attacks. The current intrusion prevention (firewalls) or detection approaches are reactive and require prior knowledge of all the attack modalities and software vulnerabilities.

In response to these problems, Sood developed a proactive risk management approach called Self Cleansing Intrusion Tolerance (SCIT). SCIT servers are focused on limiting the losses that can occur because of an intrusion. Sood's risk management process achieves this goal by limiting the exposure time of the server to the Internet. Sood believes that exposure time is a good security metric and thus uses it in his risk management approach.

Sood is a Professor of Computer Science and Director of the Laboratory of Interdisciplinary Computer Science at George Mason University, and is founder of SCIT Labs Inc. Sood is currently forming a university spin-off to commercialize this technology, which will be based on the patents that have been applied for by George Mason University.

Irving Lachow

Cyber Terrorism: Menace or Myth?

As Irv Lachow explained in his presentation, cyber terrorism is often portrayed as a major threat to the United States. Articles, books, and reports discussing the subject conjure images of infrastructure failures, massive economic losses, and even large-scale loss of life. According to Lachow, the hype surrounding this issue has outpaced the magnitude of the risk: there has not been a single documented incidence of cyber terrorism against the U.S. government. Perhaps this current trend is likely to continue, or perhaps it is just a matter of time until terrorists launch a massive cyber attack against the United States. Lachow's presentation addressed these issues by utilizing a risk management framework to explore the factors that terrorists must consider when deciding whether to pursue cyber-based attacks. His risk management framework provides an assessment of the overall risks posed by cyber terrorism today and in the next few years. Lachow's presentation can be found on SARMA's conference webpage.

Lachow is a Senior Research Professor at the National Defense University's Information Resources Management College. Lachow has extensive experience in both information technology and national security, having worked for Booz Allen Hamilton, the RAND Corporation, and the Office of Deputy Under Secretary of Defense (Advanced Systems & Concepts). ❖

About the Security Analysis and Risk Management Association

Mission

The mission of the Security Analysis and Risk Management Association (SARMA) is to promote the rapid maturation and standardization of security analysis and risk management techniques by providing an open forum for cooperation and collaboration among all practitioners. It is dedicated to providing leadership, educational programs, and certification for all security analysis and risk management professionals. By integrating government, academia, and the private sector in its activities, SARMA also helps each work together in developing more mature, standardized, and consistent methods. SARMA envisions that these methods will one day be practiced by a growing cadre of formally trained and certified professionals. The driving purpose behind SARMA's activities is to help make our nation more secure and prepared through effective, risk-based decision-making. SARMA's specific initiatives include:

- Providing an open forum for all security analysis and risk management professionals to share information, ideas, and methodologies;
- Standardizing the professional lexicon and generally accepted security analysis and risk management principles for the benefit of all security professionals;
- Supporting the professional development of members through voluntary participation in meeting minimum professional standards; and,
- Promoting the profession of security analysis and risk management as a desirable career choice, thereby creating professional opportunity.

Background

Over the past two decades, security analysis and risk management have become increasingly critical to the national and economic security of the United States. On September 11, 2001, it became important to our homeland security, as well.

Recognizing the need for a professional association to serve those responsible for analyzing and managing security risks to systems, structures, and operations from man-made threats, SARMA was incorporated in early 2006. The Association was, and remains, an all-volunteer professional association, led by dedicated professionals and experts in the field, and open to partnership with all security analysis and risk management professionals and organizations. The Association is strictly non-partisan, and strives to represent the profession and involved organizations in a fair, balanced, and independent manner.

Since its inception, SARMA has become one of the fastest-growing and best known professional associations in the security field. Yet, what makes SARMA unique is its focus on the analysis and management of a broad array of security risks. Now starting its third year in operation, SARMA is poised to grow into the security profession's most influential and forward-looking association.

Accomplishments

Thanks to the collective efforts of numerous dedicated professionals, the security analysis profession has now taken its first bold steps toward organizing with a common goal and the public good in mind. One of SARMA's first, and most ambitious, projects is to collect and document the existing knowledge of the profession through its Common Knowledge Base (CKB) Program. This Program is creating the foundation of knowledge that can be shared within the profession, as well as taught to future generations of security professionals. To facilitate the collection and sharing of this knowledge, SARMA also created the SARMApedia, a wiki-based technology that allows anyone to contribute. The SARMApedia has since expanded beyond its original purpose, and now holds over 300 articles describing methodologies,

(Continued on Page 23)

Operational Critical Infrastructure Protection: The Utilities Field Service Conference

by Joseph Maltby, Law Intern

Critical Infrastructure Protection (CIP) should be approached on various levels, including strategic and operational. The task of protecting infrastructure is too complicated to perform without some sort of overarching strategy. Operating without such a plan is a surefire method for wasting time and money. At the same time, CIP isn't all plans and mandates. The battle to protect our infrastructures will be won or lost in daily operations. This is where the ideals of CIP are translated into some sort of concrete practice.

Utilities Field Service 2008, held from May 28-30th, was a forum that focused on the field service operations of gas, electric, and water utilities. These are the day-to-day activities that sustain service for their customers. More attention given to these issues will translate to a more effective utility that offers better services to its customers, competes more effectively in the marketplace, takes full advantage of new technologies, and most importantly for the purposes of this publication, is more secure and better protected. The conference included attendees from both the public and private sectors spanning dozens of states and Canada. The attendees were largely utility executives and senior staff from various state and federal regulatory bodies. Conference presentations and discussions focused around new technologies, such as the smart grid, regulatory concerns, and disaster response. The entire first day of the conference was devoted to the smart grid, in fact, indicating that it occupies an important position in the minds of utilities' leadership.

One of the most interesting observations made repeatedly at the conference was on the dramatic changes made in the way utilities do business caused by recent worldwide and technological developments. John Baker from Austin Energy spoke on the strategic challenges of ensuring reliability when market forces across the world drive energy prices and new regulations, such as carbon limits, will change the rules of the game. He pointed out that as green technologies are becoming more popular, they will change how utilities do business. It is a notably different process to ensure reliability when significant portions of the grid are composed of renewable technologies such as wind and solar power. He also noted that distributed generation is becoming increasingly popular, meaning that the grid will be de-centralized, which poses its own series of organizational problems.

Paul De Martini from Southern California Edison, Mireille Gotsis from AT&T Mobility, and Tony DiMarco from Intergraph each spoke on the promises of new technologies for utilities. De Martini explained how the smart grid is designed not just to increase reliability but also to reduce the risk of catastrophic system failure. Gotsis, in turn, talked about the uses of wireless technology in the energy sector. She stated that the transformation of the electrical grid to a wireless system would allow for quicker system restoration after a disaster, as well as remotely monitoring both the physical and operational infrastructure. DiMarco mentioned the use of new programs to sift through data collected by the utility and find patterns that indicate a security risk or a threat to critical infrastructure. In addition, new wireless security cameras can be programmed to search for specific sets of variables which may indicate a security breach without relying on the attention of security personnel.

Tom Standish from CenterPoint Energy gave a riveting presentation on some of the possibilities for a new utility business model based on the technologies being developed today. He pointed out that new "smart" meters can be given IP addresses, making them internet accessible. This raises the question as to why utilities need to own these meters. For example, an independent company could buy the rights to a series of meters, pay the users to reduce demand, and then sell that unused power on the market, acting almost as a independent distributed generator. Electric or hybrid cars could be used as a mobile power source, moving

(Continued on Page 16)

Energy Conference *(Cont. from 15)*

electricity from different portions of the network. He noted that digitizing electrical infrastructure is an expensive process which currently has no overall set of standards, meaning that infrastructure replaced today will not only have difficulty communicating with other utilities' networks, but will also have trouble communicating with infrastructure replaced five or 10 years from now.

The second day of the conference focused on operational issues. Craig Glazer from PJM Interconnection mentioned the importance of keeping up with operational basics. He pointed out that every blackout in recent memory has been caused, at least in part, by vegetation management failures. Tony Hurley from FirstEnergy discussed the problem of data sifting. Utilities are receiving more and more data as information-gathering technology spreads, but without a good data management system this data is largely useless. He mentioned the use of software to analyze this data stream for patterns and to sift through it for the really important pieces, a process which is not dissimilar to what national security analysts do, albeit on a smaller scale.

The conference ended with a presentation I offered on behalf of the CIP Program regarding some of the cyber security implications of the shift to a smart grid. I noted that a smart grid, while increasing efficiency and responsiveness, is also more vulnerable due to its interconnections. I also spoke on the very real probability of new federal regulations regarding the electrical grid, as the North American Electric Reliability Corporation (NERC) is currently revising its cyber security standards for utilities. The importance of proper cyber security precautions cannot be overstated, especially considering most people — including relevant decision-makers — are unfamiliar with this field. This unfamiliarity was demonstrated by the fact that my presentation was the only one dealing specifically with the security aspects of the smart grid. Though, obviously, inviting me to speak represented an understanding that this topic needed to be covered. (The CIP Program is planning a workshop to speak more directly to these vulnerabilities. Information about the event will be posted on our website at a later date.) Technological literacy is spreading, but the process of protection is less a destination than a trip, as those protecting the system will always be competing with those trying to destroy it.

For more information on the Utilities Field Service event, visit http://www.wbresearch.com/utilitiesfieldserviceusa/. ❖

Panel Discussion on Public-Private Partnerships

On behalf of the CIP Program, I also participated in a panel discussion regarding public-private coordination for emergency planning and response. This gave me an opportunity to hear, firsthand, what representatives from the private sector consider most important in this area. One big question I heard repeatedly from executives managing disaster response and planning was: "How do I coordinate better with my counterparts at the state and federal government level?" This is somewhat interesting given the amount of effort government disaster planners expend to do just that.

It also underscores the importance of reaching out and making connections. I pointed out that, within disaster response and planning agencies, there is an individual responsible for coordination whose performance is measured by how many private sector representatives he/she can collect for planning and response exercises. This point was seconded by a conference participant who spoke on behalf of his state's public service commission and stated that he made it his day-to-day job to reach out to as many utility representatives as possible.

Therefore, I emphasized that if utilities have thoughts, suggestions, or concerns about their state's disaster planning framework or about the exercises they are invited to participate in at both the state and federal levels, they should speak up, because this is the kind of input that government employees want to hear. Hopefully, in time, the private and public sectors will be able to make that connection on a more regular basis, rather than trying to guess at what the other is thinking.

Legal Insights

CI/KR Public-Private Partnerships — Sharing Responsibility, Managing Risk

by Timothy P. Clancy, JD, Principal Research Associate for Law

> "Traditional national security concerns must give way to a concept of shared threats, for which responsibility must be shared between government and infrastructure owners and operators."
> *Critical Foundations: Protecting America's Infrastructures*
> Report of the President's Commission on Critical Infrastructure Protection, 1997

The concepts of shared responsibility, public-private partnership, trusted environment, and information sharing were first enshrined in the 1997 President's Commission on Critical Infrastructure Protection (PCCIP) report and remain at the core of the Nation's CIP efforts. The NIPP — the primary federal document on CI/KR security — is based on a partnership model emphasizing voluntary participation by private industry in critical infrastructure Sector Coordinating Councils (SCCs). We're all familiar with the "85%" private sector ownership figure confidently cited in nearly every CIP document since PCCIP. Whether this figure is 100% accurate or based on any in-depth analysis is debatable but, regardless, little or no infrastructure would function (critical or otherwise) without the efforts of private sector owners and operators.

When it comes to shared responsibility for CI/KR, public and private stakeholders practice some form of risk management. These risk management concepts are set forth in the NIPP — a comprehensive risk management framework that informs the development of many different infrastructure security plans, the Sector-Specific Plans (SSPs). Risk management principles include: risk identification, assessment, mitigation, and adaptation.

Implementing risk management techniques in the public sector can be wildly different than doing so in the private sector. First, the roles of the public and private sectors are fundamentally different: the public sector is responsible for overall national and homeland security and the private sector only has a general duty to take reasonable safety steps. Second, public officials have more constraints in making risk decisions; government agencies must contend with the sometimes arbitrary dictates of legislatures and can be constrained by the public's perception of risk. Private companies have more freedom to innovate, consider opportunity risk, and insure against certain risks.

To bridge this gap, public-private partnerships are at the core of national CI/KR risk management activity. Since risk is really about uncertainty, accurate and timely information about infrastructure threats and vulnerabilities is necessary for effective risk management, public and private. Without such information, risk management is at best wasteful and time consuming, and at worst useless.

From a legal perspective, public-private partnerships are strange territory. There are certainly myriad legal issues that surround these public-private activities — antitrust, conflicts of interest, open government (Freedom of Information Act) laws, government secrecy, privacy laws, tort liability, and corporate fiduciary duties. Whatever one calls them — groups, councils, task forces, or some other name — public-private partnerships are not partnerships in a true legal sense. Under the law, partnerships are for-profit business associations defined primarily by state law and are also governed by the laws of agency for tort liability purposes (except limited partnerships). Public-private partnerships in homeland security are convened

(Continued on Page 23)

The CIP Program Names a New Director

*Below is a copy of the George Mason University School of Law and CIP Program press release "**DODIG Claude M. 'Mick' Kicklighter Named Director of CIP Program**," dated July 2, 2008. Mick Kicklighter joined the CIP Program this month, relieving Dan Polsby, Dean of the Law School, who had been serving in an acting capacity since the departure of our previous director.*

Claude M. "Mick" Kicklighter, who has served for the past year as Inspector General of the Department of Defense, will become the new Director of the Critical Infrastructure Protection (CIP) Program at George Mason University School of Law beginning on July 14.

"We are delighted to welcome one of the nation's most illustrious public servants to George Mason," said Dan Polsby, Dean of the Law School. "Mick Kicklighter has the ideal combination of expertise, energy and people skills for this assignment. We look forward to his arrival with great excitement."

A retired Army lieutenant general, Kicklighter has served in a number of senior positions in the Departments of Defense, State and Veterans Affairs. Prior to being Inspector General, he was Chief of Staff to the Secretary of Veterans Affairs. In 2005, he was chosen to lead the efforts of the Departments of State and Defense in developing the Iraq/Afghanistan Joint Transition Planning Group. In 2004, he was designated as Special Advisor to the Deputy Secretary of State for Stabilization and Security Operations in Iraq and Afghanistan. He previously served as Director of the Department of Defense's Iraq Transition Team, which planned the establishment of the new U.S. Mission to Iraq. He served also as Assistant Secretary of Veterans Affairs for Policy and Planning, the Secretary's senior advisor on planning, policy research and analysis, among other issues.

As an army officer, Kicklighter commanded units at every organizational level, from platoon to division, including a stint as Commander, U.S. Army Pacific, 25th Infantry Division (Light) and the U.S. Army Security Assistance Command. In addition to numerous awards for his military service, he is a recipient of the Presidential Citizen Medal, the Eisenhower Liberation Medal, the Decoration for Exceptional Civilian Service and a two-time recipient of the Department of Defense Medal for Distinguished Public Service.

Mick Kicklighter is a graduate of Mercer University and holds a masters degree from George Washington University. He is also a graduate of the Army Command and General Staff College and the Industrial College of the Armed Forces. He was identified after a national search assisted by Leonard Pfeiffer & Company, a Washington, D.C. based executive search firm.

The Critical Infrastructure Protection Program is a part of George Mason University School of Law. The CIP Program specializes in basic and applied interdisciplinary research in critical infrastructure protection, homeland security and national security issues. The Program also produces a monthly topical publication, *The CIP Report*, that is read widely among public and private decision-makers interested in security issues.

JMU Symposium *(Cont. from 4)*

PANEL 2 – Regional Public-Private Partnership: Mid-Atlantic States All Hazards Consortium (AHC)

Panelists: *Honorable Robert Crouch, Assistant to the Governor for Commonwealth Preparedness, Moderator; John Contestabile, Director of Engineering & Emergency Services, Maryland Department of Transportation; David Lindstrom, Chief Privacy Officer, Pennsylvania State University; and Micheal Hughes, Northeast Program Development Manager, Northrop Grumman Corporation.*

According to its website, "The All Hazards Consortium was built on the belief that state/local government is ultimately responsible for the protection of the public. Based on this assumption, the AHC sees government as the 'owner of the problem.' The private sector owns most of the assets, technologies and solutions; the universities provide research and education to address the problem; and non-profit organizations provide access to information and people who are focused on a particular segment of the problem. By bringing together all stakeholder groups into regional Advisory Committees, Working Groups and ad hoc committees, and focusing on specific issues (with state government driving the needs), a powerful environment for collaboration is created to solve tough problems that require resources from every sector."
The AHC acts as a facilitator to bring the stakeholders together from nine mid-Atlantic states to share information, collaborate in addressing possible solutions to regional homeland security challenges, identify funding sources, and develop regional initiatives that produce results.

The organizers have found that the best information sharing occurs using the workshop venue. The operating slogan is "be responsive to those who own the problem." Based on the workshop deliberations, the AHC produces white papers to be shared with federal agencies and cognizant congressional staff. The white papers' recommendations form the basis for multi-jurisdictional funding proposals. Workshop topics (and subsequent white papers) have included interoperability, catastrophic evacuation planning, fusion centers, and critical infrastructure protection. In July 2008, the AHC is sponsoring a GIS workshop at Towson.

The AHC incorporates the elements of people, process, and technology, paying particular attention to people and process. It is not possible to move to the implementation phase without having people working together across jurisdictions and across disciplines. The AHC is currently addressing more than 20 region-level homeland security and emergency management issues that the member states have identified.

<u>The Role of Academe</u>
The role of higher education in the AHC includes education, research, community outreach, and government service. Universities are often affordable; modest funding can reap major benefits due to the intellectual capital available. The AHC allows higher education to connect with the people owning the problems, figuring out who has the necessary resources, and how collaborations for solutions can be created.

<u>The Role of the Private Sector</u>
Within AHC workshops, private sector representatives are willing to share their issues, needs, and challenges, as well as information, assets, technologies, and solutions. Though not a direct pipeline for business development opportunities or contracts, the AHC provides a unique listening opportunity for private business to interact with end users. The AHC provides a level playing field for contractors. This interaction allows for more intelligent requests for proposals (RFPs) to be issued and for more in-depth cross-jurisdictional collaborations.

A critical lesson from this partnership is the importance of two bedrock principles: trust and focus on priority problems. Trust must be engendered across the disciplines and jurisdictions, or they will not stay engaged. As long as focus remains on the problem and trust is maintained amongst the parties, collaboration is possible. When either of those two tenets is violated, there will be problems.

PANEL 3 – National Public-Private Partnership: The National Security Telecommunications Advisory Committee Telecommunications/Electric Interdependency

Panelists: *Dr. John S. Edwards, Nortel's Designated Representative*

(Continued on Page 20)

JMU Symposium *(Cont. from 19)*

to the NSTAC's Industry Executive Subcommittee, Moderator; Daniel C. Hurley, Jr., Director, Critical Infrastructure Protection, U.S. Department of Commerce, National Telecommunications and Information Administration, and Chair of the Communications Dependency on Electric Power Working Group (CDEP WG); and Lawrence Hale, Acting Director, National Communications System (NCS).

The President's National Security Telecommunications Advisory Committee (NSTAC) has a 25-year history of government-industry partnership with several important contributions to assure the security of the Nation's telecommunications service. Recently, NSTAC sent to the President a two-part report on the interdependency between telecommunications and electric power services. The first part, "People and Processes," covered access control measures and cooperation in the aftermath of natural and man-made disasters. The second part, discussed issues related to what the Committee described as "Long Term Outages" and addressed measures to mitigate effects, recover operations, and methods to reduce the likelihood in advance.

Both reports were based on collaboration between the telecommunications and electric power industries and the governments of Canada and the United States. Although NSTAC sponsored and led the effort, a unique collection of subject-matter experts from the telecommunications and electric power industries, and government from both countries met collegially over a two-year period. The reports were submitted to President Bush and as a result, the government established a Communications Dependency on Electric Power Working Group (CDEP WG).

Mr. Dan Hurley chairs the CDEP WG. Its mission is to research and report on issues relating to long term outages. It is a difficult problem because the longest outage our nation has had only lasted about two weeks. The CDEP WG is looking at situational awareness tools and their usefulness in coordinating with other critical infrastructure sectors. It is also looking at new technologies for backup power, including fuel cells, wind power, photovoltaics, and recovery transformers. The WG should have an initial draft report on its findings by the end of summer 2008.

NSTAC industry subcommittees are ongoing and productive. The government supports NSTAC primarily by providing information; government representatives do not get involved in deliberations. Some examples of areas being addressed by NSTAC include:

- Emergency communications and interoperability – task force established
- Assessment of dependence on GPS and implications of loss or disruption – task force established
- Global infrastructure resiliency
- Examination of legislative and regulatory developments
- Examination and report on Estonia cyber attacks
- Network security

One significant example of a public-private partnership began in 2003, when Dr. Jack Edwards was asked by then-NSTAC Chair Duane Ackerman to head an interdependency task force. NSTAC had, in the past, addressed "dependency," but not "interdependency." For instance, dependency studies had looked at the vulnerability of supervisory control and data acquisition (SCADA) systems. Mr. Ackerman asked two fundamental questions: (1) how do the telecommunications and electric power infrastructures rely on each other? and (2) how would they need to be rebuilt if they were both down for a period of time? The Interdependency Task Force first met in the spring preceding Hurricane Katrina. Katrina provided a useful case study for the group's after-action report.

This Task Force reached out beyond the telecommunications industry to include members of the electric power and other private industries and government organizations in the United States and Canada. In North America there is no distinction between Canada and the United States in electric power and telecommunications. However, there are big differences in viewpoints between the telecommunications and electric power industries concerning outages. The Task Force concluded that a very strong situational analysis tool is needed to work with fusion centers to develop a composite picture of large-scale outages.

NSTAC government-industry partnerships have demonstrated that there are major economic benefits of

(Continued on Page 21)

JMU Symposium *(Cont. from 20)*

public-private partnerships. Government interaction with industry is essential to improving the resilience of our critical networks.

Afternoon Keynote

The Honorable Alfonso "Al" Martinez-Fonts, Jr., is Assistant Secretary for the Private Sector Office, U.S. Department of Homeland Security.

As Assistant Secretary for the Private Sector Office of DHS, Martinez-Fonts described the 2002 law that created DHS, which also gave his office seven tasks to achieve. Subsequent laws over the last six years have added four more tasks, bringing the total to 11 unique mandates.

Speech Excerpt:

First and foremost, we are to advocate clearly on strategic issues for the private sector. If you are in the private sector, I'm the guy you want to know in the Department. I don't have a budget, I don't buy things, and I'm not on the procurement side.

The second thing that we do is share information and best practices. I don't generate the information. What we try to do is make sure that we can bring that information in at an unclassified level to share it with more people and businesses and to make it actionable. Do I need to put some guards on the back gate? Do I need to change the HVAC system? Do I need to stop a truck from coming into my facility? We do our best to get information out that is important to the private sector, especially information on best practices for areas such as pandemic influenza and telecommuting.

In the Private Sector Office, public-private partnerships are clearly the cornerstone of our mission, and both sides need to be present to solve homeland security problems. There is a need for a champion . . . someone who will sometimes put his neck on the line to make sure this thing gets done.

The example I will relate occurred at a border port. On one side is the port of Nogales, Arizona. On the other side is the port of Nogales, Sonora. It is one of the busiest ports on the southern border. The joke in Nogales was, as a member of [Customs-Trade Partnership Against Terrorism] *C-TPAT, it takes you two hours to get across the border. As a non-member it takes you two hours and one minute. It was clear that we needed to build infrastructure to improve the throughput of the last stretch. The projected price was $10 million. The partnership did not happen automatically — it took a lot of work and pushing to get the stakeholders together to do it, but the end result was more lanes built, shorter time frame and the cost reduced to $3.2 million.*

Another example is from Assistant Secretary [for Infrastructure Protection] *Bob Stephan. I view the Critical Infrastructure Partnership Advisory Council or CIPAC as one of the all time greatest public-private partnerships. The CIPAC is really a process under which we have created now 18 self-organized critical infrastructure councils. It is like that old Saturday Night Live, "talk amongst yourselves" routine. Go over there, bankers, and talk amongst yourselves. Go over there, energy people, and telecommunications people and so on and talk amongst yourselves. We then brought the government side together and said, if you want to talk among yourselves, you need to make sure that you include the private sector.*

In order for the CIPAC to work, it was very important to address possible problems due to the Federal Advisory Committee Act or FACA. The Secretary used his authority to exempt the entire CIPAC group from FACA. It was not a case of the government trying to hide things. If discussions at CIPAC meetings were published in the Washington Post or the New York Times, no one would talk. So we needed to have a legal structure that would exempt us from FACA and allow us to have the kind of relationship we needed among the private sector companies and most importantly the industry sector and the government. CIPAC created that protective space to do that. The CIPAC includes sector coordinating councils and government coordinating councils.

This partnership has been invaluable in enabling discussions among interdependent infrastructure communities essential to protecting our critical assets. To me this is one of the greatest examples of a public-private partnership and I have been much impressed with the enthusiasm and buy-in that we have had from all of the sectors.

Being able to create public-private partnerships, I am convinced, is the way that were are going to make this country stronger, to make it more resilient and to be able to solve the kinds

(Continued on Page 22)

JMU Symposium *(Cont. from 21)*

of issues needed to be prepared for the next attack, the next hurricane or the next incident. We don't know what it is going to be, but believe me, it is going to happen. To the extent that we can create public-private partnerships, we will be so much better off.

Synopsis - Emergent Themes

The public-private partnership examples included in the symposium illustrate the importance and strong benefits of collaboration among government, private industry, and academe in addressing homeland security challenges. Some important common themes were reinforced by the panels relating to establishment and operation of public-private partnerships and their benefits in improving system and community resilience.

1. In most cases, solutions to homeland security problems are not possible without public-private partnerships. The fact that most critical infrastructures are privately owned reinforces this theme. The government does not have the organic technical expertise needed to solve many problems.

2. Public-private partnerships improve the effectiveness of solutions. The private sector brings innovation, management expertise, and the profit motive to the table. The government brings authority, management expertise, high-level perspective, and funding to the table. Both are needed to achieve best solutions to homeland security problems.

3. Public-private partnerships reap benefits at all levels, federal, state, and local.

4. Bringing state government, business, and academic communities together has resulted in much better informed and comprehensive planning for regional emergency preparedness.

5. Public-private partnerships provide mutual, win-win benefits to the public and private sectors. Examples were given illustrating the private sector becoming a "force multiplier" for the public sector. The public sector helps the business continuity of the private sector.

6. Outcomes are both people-driven and process-driven. It is helpful to have goals and metrics related to the outcomes.

7. Public-private partnerships result in cost savings.

8. Public-private partnerships are not easy to establish and sustain. The key is finding where public interests lie and where private interests lie and then finding common ground. The private sector participates in three roles: as a victim, vendor, and partner. The partner role is the most challenging.

9. Public-private partnerships require mutual trust, a common-objective, and organization skills to get people and groups to work together over the long periods needed to solve homeland security problems. Relationships need to be based on mutual benefit and respect rather than being externally forced. A culture of collaboration is essential and the partnership needs to build it, sustain it, and take pride in it.

10. Partnerships require sharing resources.

11. Professional societies are often a very important venue for coordination, information exchange between the public and private sectors, and the establishment and life of public-private partnerships.

12. Public-private partnerships require good communication. Partners need to develop a common language that oftentimes is not there to begin with due to differences in communities and disciplines among the participants.

13. Information sensitivity is a major hurdle in establishing public-private partnerships. Means must be developed to protect critical private sector information from disclosure.

14. Partnerships work when participants recognize that their citizenship extends far beyond narrow self-interest.

15. Public-private partnerships benefit from including academe at the table. Modest funding can reap major benefits due to the intellectual capital that is brought to bear. ❖

Supply Chains *(Cont. from 11)*

different legal systems. They must add managing the risk of disruptions to their supply chain from global threats as well. Such risks can be managed through a process of prioritizing risks and threats, emergency planning and preparedness, and testing and exercising risk management practices to determine how to best protect the supply chain of an enterprise. This is a growing field and much work remains to be done. Yet, an investment several years ago might have put in place the mechanisms needed to identify the most obvious potential threats and enable decision-makers to have compensated for them in their business models. For example, those companies that took high fuel prices into account several years ago are the ones who are struggling less to make ends meet today.

It would be foolhardy, as well as impossible, to try and put the genie back in the bottle and dispense with globalization. Outsourcing, global supply networks, and information technology bring with them too many benefits to be discarded. But there is no harm in approaching the world with open eyes. ❖

About SARMA *(Cont. from 14)*

key terms, R&D efforts, best practices, and a listing of experts and key organizations.

Currently the SARMApedia contains the following five sections:

- Common Lexicon
- Encyclopedia of Security Analysis Methods
- Research & Development in Risk Management
- Who's Who in Security Analysis
- Generally-Accepted Risk Assessment Principles (GARAP)

For more information about SARMA, and its activities and projects, please visit SARMA's website at http://www.sarma.org, and the SARMApedia at http://www.SARMApedia.org. ❖

Legal Insights *(Cont. from 17)*

usually as the result of government directives, such as Homeland Security Presidential Directive-7, but remain voluntary associations with government serving as a facilitator or coordinator.

Of course, government agencies can and do act as regulators within certain authorities and the dividing line between coordination and regulation can be vague, inhibiting participation by private sector stakeholders. Also, the expectations of the public and private sectors can be very different, particularly when it comes to information sharing. Often, both sides believe that the other has a huge reservoir of data that can be tapped, when in reality either the information doesn't exist or if it does, it is buried, scattered, inaccessible, or simply unknown.

For many public-private partnerships it comes down to trust, a quality that cannot be mandated or engineered. Developing trust can be a decade-long contact sport and often depend on individual personalities and experiences.

The key for the federal government, the private sector, and the NIPP framework is to go beyond mere personality and develop a predictable, repeatable system of two-way communication between industry and the government. To achieve this, effective measures of CI/KR public-private partnership performance must be developed and shared. While each sector partnership will be unique, there are universal metrics that can be analyzed to judge partnership effectiveness and can be incorporated into the NIPP model.[1] We hope to have greater discussions of metric development for CI/KR partnerships in future editions of *The CIP Report*. ❖

[1] See, presentation by Robert Weaver, former Special Agent in Charge, United States Secret Service, "2008 CI/KR Public Private Partnerships: The Path Forward," available at http://www.nlectc.org/training/nij2007/weaver.ppt.

Paper on Foreign Investment in Critical Infrastructure

The Organisation for Economic Co-operation and Development (OECD) has released a public version of a paper co-authored by Maeve Dion, Legal Research Associate with the CIP Program. The paper, titled *Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security*, can be found on the OECD website (PDF file). This paper was prepared at the request of the OECD Secretariat, under the Directorate for Financial and Enterprise Affairs. Related work can be found on the OECD website, in the section on "Preventing Investment Protectionism."

ERM *(Cont. from 9)*

The need for collaboration among the numerous departments of a company is also essential to security management. Further, understanding where security risks lie and the benefits to the company of addressing those risks is needed to implement proactive SRM.

With better business cases and enhanced SRM, Talbot relayed that SRM can serve as a profit driver for enterprises. At optimal maturity, proactive SRM will provide companies with competitive advantages and improve resilience. In sum, companies can benefit greatly from integrating security risk management with their business practices.

For copies of the presentations given by Liscouski and Talbot, visit http://sarma.org/events/pastevents/2ndnationalconfere/2008sarmaconferenc/. ❖

Risk Management *(Cont. from 10)*

using a common risk method, process and tool to measure security risk at the local, regional, and national levels. The MSRAM Software/Process includes:

1. List Targets
2. Score Maximum Consequence
3. Score Scenario Risk
4. Analyze Results & Generate Reports
5. Alternatives Analysis ❖

The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The CIP Program is funded by a grant from the National Institute of Standards and Technology (NIST).

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

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1