

AND HOMELAND SECURITY

AUGUST 2010 CIP/HS UPDATE

10110

EDITORIAL STAFF

EDITORS Devon Hardy Olivia Pacheco

JMU COORDINATORS Ken Newbold John Noftsinger

> **PUBLISHER** Liz Hale-Salice

Contact: <u>CIPP02@gmu.edu</u> 703.993.4840

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu In this month's issue of *The CIP Report*, we provide an update on the Center for Infrastructure Protection and Homeland Security (CIP/HS), including information on current projects as well as past and future conferences.

First, we provide a brief overview on the mission and School of Law the recent activities of CIP/HS. Next, we provide information on a collaborative project between CENTER George Mason University and the Korean Electric for INFRASTRUCTURE PROTECTION Power Company (KEPCO). Then we provide a and summary on a symposium we recently co-hosted with HOMELAND SECURITY the InfraGard Nations Capital Members Alliance (INCMA). We also discuss our involvement with the newly formed Cybersecurity Board of Advisors at the U.S. Department of State Office of Diplomatic Security. We describe a workshop, sponsored by the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate, Infrastructure and Geophysical Division, which we hosted on the challenges associated with modeling, simulation, and analysis. Then we summarize the events that occurred at a conference, sponsored by PricewaterhouseCoopers (PwC), on information sharing and risk management. We co-hosted this event with the Security Analysis and Risk Management Association (SARMA). We also co-hosted an event with SARMA on achieving enterprise resilience. We include information on a joint George Mason and DHS initative on Critical Infrastructure Higher Education Programs. The remarks of James Madison University (JMU) President, Linwood H. Rose, on safe, secure, and sustainable facilities at the Institute for Infrastructure and Information Assurance (IIIA) 5th Annual Spring Symposium are also included. Finally, we announce the Forth Annual Security Analysis and Risk Management Association (SARMA) Conference.

DUTGOING MAIL

We hope you enjoy this issue of *The CIP Report*. We thank you for your continued support and feedback.

ichlighten

Mick Kicklighter Director, CIP/HS George Mason University, School of Law

The Center for Infrastructure Protection and Homeland Security (CIP/HS)

There are many new endeavors and ideas that have come about since the last CIP/HS update and we are pleased to share these with you. In addition to the publication of the monthly newsletter, *The CIP Report*, CIP/HS supports a number of programs and projects to achieve its mission. While a majority of these programs and projects will be discussed in detail later in this issue, there are several projects we would like to highlight.

CIP/HS has gathered an impressive array of experts in the field of infrastructure protection and homeland security to make up the Fellows Program. The CIP/HS Fellows Program includes individuals that provide expertise in the areas of bioterrorism, counterterrorism, disaster preparedness, education, energy, infrastructure protection, intelligence, law enforcement, military strategy, and public health. These prominent professionals have assisted staff with numerous publications and projects. In fact, several CIP/HS Fellows have supported and/or written for various issues of The CIP Report, discussing such topics as education, international infrastructure protection, biosecurity and biosafety, and nuclear energy. This program adds a significant value to the work done by CIP/HS.

We have invited two academic professors to conduct research at CIP/HS. Dr. Duminda Wijesekera, an Associate Professor in the Department of Information and Software Engineering at George Mason University, joins CIP/HS for the next year to conduct research in the fields of information technology and energy. He will also serve as Acting Program Manager of the Energy Program at CIP/HS. Professor John W. Bagby, Co-Director of the Institute for Information Policy in the College of Information Sciences and Technology at Pennsylvania State University, worked at CIP/HS for the summer, focused on educational initiatives.

We have also been working with European Command (EUCOM) to discuss the various challenges involved with cyber defense. This is a relatively new project, but we hope that this collaboration will create future opportunities.

We also recently co-hosted two workshops with the George Washington University Office of Homeland Security on Experts in Medical Surge: Community Medical Resiliency in Disasters. The first workshop took place at CIP/ HS while the second workshop occurred in Denver, CO. Representatives from Federal, State, and local governments participated in these two workshops, which fostered enthusiastic discussion on the obstacles surrounding medical resiliency in disasters. The organizers of the event are currently writing the final report, which will discuss both the obstacles and the proposed solutions to medical resiliency in disasters.

On July 29, we had the pleasure of meeting with the distinguished members of our Advisory Board. General William Reno, the Chair of the CIP/HS Advisory Board, opened the meeting with comments about the evolution of CIP/HS since the last Board Meeting held in December 2008. His remarks were followed with introductions by the Dean of the Law School at George Mason University, Dan Polsby, the Director of CIP/HS, Lieutenant General Mick Kicklighter (Ret.), and Admiral Patrick Dunne. The CIP/HS Program Managers and staff members presented on projects and conferences. During the meeting, Board members engaged in lively and energetic discussion on issues such as nuclear energy, cybersecurity, and education and training. General Reno closed the meeting with ideas and suggestions for CIP/HS to move forward to better serve this Nation in its quest to provide the public and private sectors as well as academia with the knowledge to improve international and national security. Our renowned board members provided us with invaluable guidance and recommendations to realize this ambitious goal.

We hope that you find this issue of *The CIP Report* valueable. We invite each of you to provide comments on this issue and, most importantly, we encourage you to reach out to us so we can work together to enhance the infrastructure of this unique and resilient Nation.

George Mason/KEPCO International Nuclear Graduate School (K-INGS): Nuclear Power Engineering Program

As the demand for nuclear technology continues to grow, Korea gained significant notoriety in the energy field when the Abu Dhabi Government selected a consortium of Korean firms to build what will be the premier facilities for the generation of atomic power in the United Arab Emirates. They are also pursuing opportunities in Turkey, Indonesia, India, and the People's Republic of China. According to the Korea Herald, the Korean government plans to invest US\$355 million over the next seven years to improve and further its efforts to export its nuclear technology.¹ The government also plans to bolster human resource capability in the field by dedicating a graduate school to the subject of atomic power.

The Korea Electric Power Corporation (KEPCO) of South Korea plans to open the world's first graduate school focusing exclusively Artist's rendition of the KEPCO International Nuclear Graduate School, located in the KORI Nuclear Power Plant Complex.



on nuclear power plant studies in 2012. KEPCO is an integrated electric utility company engaged in the transmission and distribution of electricity in Korea, and recognizes opportunities to enter into the global nuclear power plant market.



(Far left) Dr. KunMo Chung and (far right) Dale Klein. *Photo courtesy of Dale Klein.*

KEPCO and its four affiliates will support the financing and training of the teaching staff, and host a mix of highlyqualified students at the KEPCO-International Nuclear Graduate School (K-INGS). The school will admit a total of 100 nuclear energy specialists, including 50 Korean and 50 International students each year. Its two-year program will be conducted in English.

Groundbreaking ceremonies took place on July 22, 2010 for the new K-INGS facility located adjacent to the four-reactor Kori nuclear power plant in Gori (a suburb of the southern port city of Busan). The proximity to this working nuclear facility will enable students to gain hands-on experience in the applications of nuclear technology.

Currently, CIP/HS Distinguished Fellow, Dr. KunMo Chung, is leading the establishment of K-INGS. CIP/HS and George Mason will support K-INGS to

(Continued on Page 18)

¹ *The Korea Herald*, KEPCO to Open Graduate School on Nuclear Power Studies, March 30, 2010, available at: http://www.koreaherald.com/business/Detail.jsp?newsMLId=20091231000002.

The Virginia Fusion Center and Office of Commonwealth Preparedness

On the evening of April 14, 2010, CIP/HS and InfraGard Nations Capital Members Alliance (INCMA) co-hosted an event on the Virginia Fusion Center and commonwealth preparedness. The event, held at the George Mason University Arlington Campus, brought together infrastructure protection industry experts and stakeholders from Federal, State, and local agencies.

Captain Steven Lambert of the Virginia State Police was the first of two speakers. Captain Lambert's presentation introduced the missions and functions of the Virginia Fusion Center (VFC). The VFC was created as a partnership between the Virginia State Police and Virginia Department of Emergency Management. The VFC's primary mission is to fuse together resources from Federal, State, and local agencies as well as private industries to facilitate information collection, analysis, and sharing in order to prevent terrorist attacks and criminal activity in the Commonwealth. Its secondary mission, in support of the Virginia Emergency Operations Center, is to centralize information and resources to provide a coordinated and effective response in the event of an attack.

The VFC achieves its twofold mission through an extensive partnership with the intelligence community, Federal and State agencies, first responders, and the private and the public sectors. Based on information gleaned from this network, the VFC produces numerous products including tactical briefings, intelligence bulletins and reports, and threat assessments.

Speaking directly to the industry experts at the event, Captain Lambert stressed the VFC's need for improved automated database search capabilities. Currently, the VFC manually searches some 19 databases. The VFC would greatly benefit from technology that could combine these disparate databases and automate the searches.

Mike McAllister, Deputy Assistant to the Governor for Commonwealth Preparedness, was the second and final speaker of the evening. Mr. McAllister discussed what Virginia is doing to protect the 18 critical infrastructure and key resources (CIKR) sectors. In particular, Mr. McAllister highlighted the Commonwealth of Virginia's Critical Infrastructure Protection and Resiliency Strategic Plan (VCIPRSP).

The VCIPRSP is a counterpart to the Department of Homeland Security's (DHS) National Infrastructure Protection Plan (NIPP). The VCIPRSP and NIPP provide unifying structure for integrating existing and future CIKR protection efforts and resiliency strategies. Specifically, the objectives of the VCIPRSP include: understanding and sharing information about terrorist threats and other hazards with CIKR partners; building partnerships to share information and implement CIKR protection programs; implementing a long-term risk management program; and maximizing the efficient use of resources for CIKR protection, restoration, and recovery.

The Commonwealth seeks to realize the objectives of the VCIPRSP by partnering with DHS, local governments, and the private sector. Through local outreach programs, the Office of Commonwealth Preparedness develops a framework to enhance sector partnership and promote cross-sector planning, collaboration, and information sharing for CIKR protection involving all levels of government and private sector entities.

The evening marked the first event co-hosted by CIP/HS and INCMA. INCMA is the local chapter of InfraGard, which is an information sharing and analysis effort that serves the interests and combines the knowledgebase of a wide range of members that include the Federal Bureau of Investigation and other Federal agencies, businesses, academic institutions, State and local law enforcement agencies, and the public. CIP/HS hopes to host similar events with INCMA in the future, as well as support the VFC

(Continued on Page 18)

Cybersecurity at the U.S. Department of State: Bureau of Diplomatic Security Leading Efforts to Combat Cyber Threats

The U.S. Department of State's Bureau of Diplomatic Security (DS) is responsible for protecting the Department of State's vast worldwide network of critical assets — people, facilities, and information technology (IT) systems. The challenge is daunting and complex. In today's globally networked world, the Department of State's information networks carry a range of highly sensitive information — national security and trade secrets and personally identifiable information. Security is at a premium, with the security threat to the Department of State's IT systems rising substantially. In 2009, according to DS, there were 3 million intrusion events, 308,000 instances of computer viruses, and 525 million spam emails across the Department of State's IT systems.¹

At the same time, these networks must be highly robust and reliable so that this information is available for global operations 24/7. In addition, Secretary of State Hillary Clinton has been aggressively promoting the use of e-Diplomacy, Web 2.0, and social networking tools to advance its mission in the 21st century while also advocating for a free and open Internet.

This Information Age security versus availability conflict was a perennial concern even before the first IT databases and networks were created. However, as Moore's Law continues to push exponentially the power and speed of modern microprocessors and drastically reduces the costs of data storage, these tradeoffs will only grow. These are tradeoffs faced by individuals and organizations large and small every day. However, the mission of the Department of State — diplomacy and promoting democracy and freedom — makes these tradeoffs particularly acute and tough to balance.

Diplomatic Security is responsible for overall cybersecurity operations at the Department of State and operates a round-the-clock Computer Incident Response Team (CIRT) to identify threats and respond to intrusions. DS also conducts testing and analysis of software applications and promotes overall cybersecurity awareness across the Department of State. In addition, DS works very closely with the Bureau of Information and Resource Management (IRM), which manages the Department of State's overall IT infrastructure and enterprise architecture. Working together, DS and IRM have been awarded the Frank Rowlett Award from the National Security Agency twice in the past six years for achievements in information assurance, the highest award for cybersecurity in the federal government.² A key element of this partnership has been the development of a highly successful Site Risk Scoring System to identify vulnerabilities and take proactive steps to reduce cyber risks across the 370 Department of State locations, including all embassies and consulates worldwide.

Mick Kicklighter, Director of CIP/HS, is a member of a recently formed Cybersecurity Board of Advisors for DS that provides DS with a senior-level group of outside experts to address new and emerging issues in cybersecurity. Participating in the group are key officials from IRM, including the Department of State's Chief Information Security Officer John Steufert, who has been a leader in information security risk management practices within the Federal government.

Tim Clancy, Senior Program Manager for Cybersecurity at CIP/HS, has been privileged to participate in the discussions of the Advisory Board. While the group is just getting off the ground, it has provided a useful forum for discussing emerging issues in cybersecurity; such as the challenges of operating in a cloud computing environment, better integrating security operations center and network operation centers, and

(Continued on Page 18)

¹ Diplomatic Security 2009 Year in Review: Focus Forward, available at http://www.state.gov/documents/ organization/139314.pdf.

² See: http://www.nsa.gov/ia/ia_at_nsa/rowlett_awards/award_recipients.shtml.

Research Challenges in Modeling, Simulation, and Analysis: A Department of Homeland Security Workshop at George Mason University

Improving homeland security is built around risk: understanding the threats, vulnerabilities, and consequences posed by natural and man-made hazards. However, as societies become more dependent upon networked infrastructures, the consequences of a single event can be large-scale, complex, disruptive, and sometimes catastrophic. These complex events remain difficult to predict and understand even for regularly occurring natural hazards such as hurricanes and earthquakes. Modeling and simulation technologies are critical to understanding the risks flowing from complex disruptive events.

Recently, CIP/HS hosted a Workshop on Grand Challenges in Modeling, Simulation, and Analysis (MS&A) for Homeland Security, sponsored by the Department of Homeland Security Science and Technology (DHS S&T) Directorate, Infrastructure and Geophysical Division. The workshop was one of a series of workshops sponsored by DHS S&T under the leadership of Dr. Nabil Adam of DHS. An earlier workshop in 2008 hosted by the Virginia Modeling and Simulation Center (VMASC) in Virginia resulted in a December 2008 report that identified key needs and challenges for the use of MS&A for homeland security.

The 2010 workshop at George Mason was an extension of this effort and provided a forum for representatives from Federal agencies, including the Department of Defense (DoD) and DHS, to present their strategic vision of MS&A. These visions focused on the threats posed to critical infrastructure from complex, large scale, multi-faceted events as well as the cascading effects flowing from such events. Workshop attendees sought to assess the current, stateof-the-art technology in MS&A, identify challenges, and develop strategies for the development, deployment, and use of MS&A.

Dr. Jim Kadtke, CIP/HS Senior Fellow and member of the workshop Steering Committee, led the first workshop panel. Dr. Kadtke's presentation and subsequent panel examined different government approaches to uses of MS&A for infrastructure protection focusing on threats and opportunities posed by an increasingly ubiquitous sensed and networked world. Appropriate use of MS&A technologies, Dr. Kadtke noted, can help organizations: collect and analyze vast information flows; find patterns; model complex systems and behaviors; provide timely, actionable decision support; inform policy and regulation; and support collaboration, consensus building, and outreach.

The event also allowed researchers from academia, industry, and national laboratories to assess and propose solutions to research and development challenges. Also, key subject matter experts, homeland security practitioners, and State/ local representatives discussed their perspectives on the use of MS&A and its future development needs. Highlights of the workshop included presentations from a number of international experts from Europe and Australia on the use of MS&A in their respective nations. Of particular note were presentations by Australia's Critical Infrastructure Protection Modelling and Analysis Program (CIPMA) and Italy's Lombardy Region Administration that described unique public/private partnerships and the use of MS&A to overcome data gaps and understand interdependencies among private infrastructures in their respective regions.

In addition to the international flavor of the workshop, the event also enabled George Mason experts to present on new ideas and concepts for MS&A. Dr. Janusz Wojtusiak, Director of the Machine Learning Laboratory in the George Mason College of Health and Human Services, and Dr. Stephen Prior, CIP/HS Fellow, centered on the use of machine learning technologies to improve data collection and address data gaps in critical infrastructure protection. Dr. Wojtusiak is working with Dr. Prior on applying machine learning techniques to pandemic flu outbreaks.

(Continued on Page 19)

The Relevance of Risk Management and Information Sharing to Homeland Security

On March 30, 2010, CIP/HS cohosted a one-day policy forum entitled The Relevance of Risk Management and Information Sharing to Homeland Security with the Security Analysis and Risk Management Association (SARMA). While the event, sponsored by Pricewaterhouse Coopers (PwC), was delayed by the largest blizzard to hit the Washington area in 50 years, it managed to successfully bring together a wide range of experts from academia, government, and the private sector.

David Maurer, Director of the Homeland Security and Justice Program at the U.S. Government Accountability Office (GAO), provided the morning keynote address. In his thought-provoking presentation, he discussed the application of effective riskmanagement and informationsharing principles to homeland security. He noted that DHS has improved its cohesiveness and matured as a department, but that many of its 22 agencies still maintain their own institutional cultures. He stressed the importance of finding a unified mission for DHS, fostering a common internal culture, and improving coordination between agencies.

In his concluding remarks, Mr. Maurer emphasized that the Federal government lacks an informationsharing roadmap, and a system of responsibility for dealing with security issues. Athough DHS agencies have made some progress in trying to implement such a roadmap, he noted, there are also currently no metrics, accountability, or clear lines of authority. He also



(Left to Right) Kerry Thomas, President of SARMA; Jack Kelly, Policy Analyst at the Office of Management and Budget (OMB); and Joseph Kull, Director at PwC. *Photo courtesy of Liz Salice.*

noted the need for guidelines and training, and for better sharing of terrorism intelligence.

The first panel, moderated by Jack Johnson, Partner at PwC Washington Federal Practice, was devoted to Federal Program Risk Management. Jack Kelly, Policy Analyst at the Office of Management and Budget (OMB), opened with a discussion on OMB Circular Number A-123, which defines management responsibilities for internal controls in Federal agencies. In a subsequent discussion of internal controls, Joseph Kull, Director at PwC, noted their vital role in the development of policies and procedures, which in turn allow an organization to fulfill its mission, strategy, and objectives. He further stressed that, in order to succeed, an agency must have a clear mission, an objective (long-term goals and the activities needed to achieve them), benchmarks, metrics, policies and procedures in place. It also must constantly monitor and fine-tune its programs, and employ grants as an important means of gauging results in measurable ways that can be communicated to key stakeholders.

Elaborating on this discussion of grant programs and metrics, Kerry Thomas, President of SARMA, stated that today there is an inability to answer the following question: how much safer are we? He asserted that since 9/11, there have been more than \$30 billion in grants to secure the homeland, yet the grant-making process still does not have an effective means of determining the effectiveness of these funds on reducing risk. Mr. Thomas also suggested several

(Continued on Page 8)

Information Sharing (Cont. from 7)

approaches for doing things differently. First, he indicated there is a need for a common risk management framework and lexicon. Second, there is a need for a common governance structure to prevent "stovepiping." Challenges include the need to better communicate risk and the need to better manage resources.

The second panel, which focused on Cyber Risk Mitigation and Management, was moderated by Timothy Clancy, Senior Program Manager of Cybersecurity at CIP/ HS. Rear Admiral Michael Brown, Deputy Assistant Secretary for Cybersecurity and Communications at DHS, began the discussion by stating that the mission of his office is tied to the intelligence community, DoD, and the private sector. He noted that cybersecurity is one of five mission areas highlighted in the Quadrennial Homeland Security Review (OHSR). He also mentioned the need for technical expertise, the need to take advantage of changes in technology, a skilled and trained workforce that understands the threat and the technology, and the freedom to allow the workforce to be innovative. With regard to transnational threats, Adm. Brown stressed the need for global situational awareness; the need to work with law enforcement and intelligence partners; international cooperation; the involvement of the private sector in public-private partnerships; and the establishment of rules and responsibilities and the ability to deal with cyber threats.

Pablo Martinez, Assistant Special

Agent in Charge of the Criminal/Investigative Division at the U.S. Secret Service, asserted that because cyber crime is transnational, it poses logistical challenges to law enforcement agencies trying to investigate such crimes. He called for developing relationships with law enforcement counterparts overseas and with the private sector. He also talked about the role of the Internet in cyber crime, and about how every Secret Service Academy student now receives several weeks of instruction in the subject. He mentioned that the Secret Service is working with and providing key resources to State and local officials. He stressed the importance of teaching people how to use technology and of using clear terminology to help judges and juries understand the nature of cyber crimes.

General Robert Elder, Research Professor of Electrical and Computer Engineering at George Mason University, discussed the need to acknowledge the vulnerabilities and the current lack of resiliency in systems. He discussed how the military studies previous incidents in order to understand their causes as part of a broader risk management process. When discussing the transnational threat, he suggested the need to focus on the behaviors of the

Luncheon keynote Michael Belinde, Staff Director of the House Homeland Security Committee's Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment.

Photo courtesy of Liz Salice.



system. He supported the establishment of a unified Cyber Command structure at DoD, but also expressed concern about the magnitude of the challenges facing its leaders.

The third panel, Information Sharing, was moderated by Phil Lacombe, President and Chief Operating Officer at Secure Mission Solutions and Board Chairman of SARMA. Dr. Kevin F. McCrohan, a Professor in the School of Management at George Mason University, opened the discussion by providing a tactical perspective on information sharing. The quicker

(Continued on Page 9)

THE CIP REPORT

Information Sharing (Cont. from 8)

actionable information moves through the system, the more successful the homeland security enterprise will be in developing the proper response. He noted that the private sector generally reacts faster than the public sector, and stressed the need for training to clarify the importance of information sharing and speed communications.

Mr. Stewart Baker, Former National Security Agency General Counsel and Former Assistant Secretary (Under Secretary) for Policy at DHS, provided a historical overview of poor communications between the various intelligence agencies, noting that matters had greatly improved since September 11. However, he pointed out that walls that had come down in recent years were slowly being rebuilt, most notably by the Department of Justice attempting to try suspected terrorists as criminals. Mr. Baker emphasized the importance of senior leadership compelling agencies to continue the hard work

of breaking down communications barriers and preventing their reestablishment.

Nathan Sales, an Assistant Professor at the George Mason University School of Law, echoed the panel's belief that, despite some successes over the past decade, informationsharing continues to face significant obstacles. Jostling between agencies for influence over decision-makers has created a zero-sum game, with military and civilian intelligence agencies worried other agencies are free-riding off their work and then getting credit for intelligence breakthroughs. Agencies' self-image as autonomous entities has created a defensive bias against outside interference that encourages a turf warfare mentality.

Jack L. Johnson moderated the last panel of the day, Lessons Learned, in which the impressive array of panelists summed up discussions from the earlier panels. Mr. John Paczkowski, Vice President for



(*Left to Right*) Phil Lacombe, President and Chief Operating Officer, Secure Mission Solutions; George Foresman, Former Under Secretary for Preparedness at DHS and Director of SARMA; Tina Gabbrielli, Director of Risk Management and Analysis at DHS; and John Paczkowski, Vice President for Emergency Management at ICF International. *Photo courtesy of Liz Salice.*

Emergency Management at ICF International and Executive Vice President of SARMA, noted that information sharing during crisis response and disaster operations remains a significant problem. The absence of a common architecture and continued challenges in implementing interoperable voice and data systems and interagency protocols makes it difficult for states and localities to develop a common and relevant operating picture and interface effectively with Federal agencies to achieve essential collaboration and unity of effort. Mr. Paczkowski said that stronger Federal support is needed to develop a unified national architecture and common standards for operational decision-making in crisis situations.

Picking up the discussion from the earlier panels, George Foresman, Former Under Secretary for Preparedness at DHS and Director of SARMA, agreed that effective risk management required improved information-sharing, but he also

pointed out that informationsharing requires benchmarks by which progress can be measured. The issue, he said, is not what needs to get done but how it gets done. He pointed out that planners sometimes overemphasize theory at the expense of practical results, and he emphasized the need for generalists to understand the homeland security enterprise in proper context and from a broader perspective.

Phil Lacombe took a slightly

(Continued on Page 19)

Achieving Enterprise Resilience: The Convergence of Government and Private Sector Risk Management Interests Across the Homeland Security Enterprise

On June 17, CIP/HS and SARMA co-hosted a conference on "Achieving Enterprise Resilience: The Convergence of Government and Private Sector Risk Management Interests Across the Homeland Security Enterprise." The following is a summary of the keynote addresses and panel discussions.

Todd M. Keil, Assistant Secretary for Infrastructure Protection at DHS, was the day's first keynote speaker. After emphasizing that, by and large, the Nation's private and public institutions understand the importance of resilience, he called for a new national effort that "pays special attention to where our critical infrastructure is — regional and local communities."

Turning to the question of what the risk management community can do to help achieve this goal, Mr. Keil stressed the importance of developing "better decision support tools" that create "defensible analysis" for decision makers at all levels. He noted a number of important new efforts to push support out to State and local partners, including a new Regional Resiliency Assessment Program to engage and inform regional partners about the interdependencies of critical infrastructure; applied research in modeling, simulation, and analysis; and an "Infrastructure Protection in a Box" program for fusion centers to support local homeland security efforts.

The first panel of the conference, moderated by John Paczkowski, focused upon Government Perspectives. Robert Kolasky, Assistant Director, Risk Governance and Support Division, Office of Risk Management and Analysis, National Protection & Programs Directorate at DHS, opened the discussion by emphasizing that DHS understands that "homeland security is risk management," noting that Secretary Napolitano recently signed a policy statement for Integrated Risk Management (IRM). The policy statement establishes IRM as a fundamental concept that will guide the department's risk management efforts across the homeland security enterprise. This policy, according to Kolasky, squarely embeds risk management into the overall workings of the department and sets the executive mandate to build a program to improve the enterprisewide approach.

He noted that the Office of Risk Management and Analysis (RMA) at DHS has responsibility to administer and promote the implementation of the Secretary's policy by working with the department's Risk Steering Committee, which is made up of all the major components of DHS. As such, RMA has begun a benchmarking study of how enterprise risk management is applied at large organizations in both the public and private sectors. This study has led to a number of observations, including: that executive-level support for risk management policies is essential; that there needs to remain significant flexibility and variations in risk management standards; and that risk management must always be tied to strategic planning.

Mr. Kolasky offered four areas of

(Continued on Page 11)



Todd M. Keil, Assistant Secretary for Infrastructure Protection at DHS. *Photo courtesy of Liz Salice.*