THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 9 NUMBER 2

AUGUST 2010 CIP/HS UPDATE

Contact: CIPP02@gmu.edu
703.993.4840

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.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, we provide a brief overview on the mission and the recent activities of CIP/HS. Next, we provide information on a collaborative project between George Mason University and the Korean Electric Power Company (KEPCO). Then we provide a summary on a symposium we recently co-hosted with 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.

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

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, counter-terrorism, 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.

Artist's rendition of the KEPCO International Nuclear Graduate School, located in the KORI Nuclear Power Plant Complex.

The Korea Electric Power Corporation (KEPCO) of South Korea plans to open the world's first graduate school focusing exclusively 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 highly-qualified 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, state-of-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 co-hosted 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 risk-management and information-sharing 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 information-sharing 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 noted the need for guidelines and training, and for better sharing of terrorism intelligence.

(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.

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 (QHSR). 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)

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, information-sharing 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 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 information-sharing 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.

(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.

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 enterprise-wide 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.*

Resilience Conference *(Cont. from 10)*

needed improvement from the risk management community. First, he stressed the importance of "bridging the gap" between analysts and decision-makers, such that the producers of risk information can share it effectively with the consumers of the information. Second, Mr. Kolasky noted that risk analysts must develop an appreciation of simple analysis for complicated problems. The simpler the answer, the more likely it is to be transparent and defensible, and thus the easier it will be for the decision-maker to adopt. Third, risk analysts must better appreciate how their efforts impact the bottom line, because decision-makers tend to be most responsive to arguments that demonstrate achievable results. Finally, Mr. Kolasky called for the development of incentives and standards of excellence to build the human capital needed to support integrated risk management for homeland security.

Thomas DiNanno, President of Republic Consulting Group, continuing on the theme of needed improvements in the risk management community, said he had noticed a disconnect between those responsible for large regional infrastructure and those in Washington responsible for overseeing risk management programs. Having left the government for the private sector, Mr. DiNanno said he was sometimes stunned to hear security managers at the local or corporate level say they had never heard the names of certain critical Federal risk management officers.

Mr. DiNanno also pointed to the convergence of multiple regulatory schemes as an area of ongoing confusion and misunderstanding at the State and local level. Fixing the problem will not be easy because it requires multiple willing partners, he said, but not doing so undermines DHS's credibility as a single agency. Mr. DiNanno also suggested the creation of a trade association for the critical infrastructure protection community to help resolve these issues and advance the community's interests.

Mr. Paczkowski began his remarks by noting that since September 11, the homeland security community has been steadily "climbing the maturity curve" on the application of risk management concepts. While risk management principles were initially absent from security planning, he said, they are gradually becoming essential elements of more structured and deliberate planning for homeland security and preparedness. He said that State emergency management directors and homeland security advisors are increasingly grappling with how best to assess and manage risk as they work through their own planning processes, the identification of needed capabilities, and the allocation of limited State and local funding and Federal grant assistance.

Corey Gruber, Assistant Deputy Administrator for Federal Emergency Management Agency (FEMA's) National Preparedness Directorate, provided the mid-morning keynote address. He focused his talk on ways that risk management analysts can improve communication with decision-makers who must make choices within a constrained political environment. Policy suggestions must be "understandable and communicable," he said, and they must be tailored to helping the decision-maker achieve his own goals. Since political appointees often stay in their offices for only a few years, detailing short-term achievable benchmarks can make a critical difference.

The last panel, moderated by Marc H. Siegel, Commissioner, Global Standards Initiative at ASIS International, focused upon Private-Sector Perspectives, Standards Development & Case Studies. Dr. Siegel began his remarks by noting that the emergence of resilience as a key concept is being driven by a growing recognition that dividing up homeland security issues into different silos of security management, crisis management, continuity management, and recovery management does not work and is unnecessarily expensive.

The development and growth of international standards is a major part of this effort, and he warned conference participants that they have to be engaged in the discussion or risk not being heard at all. Time after time, he said, Americans fail to show up and participate in international discussions about risk management and business continuity standards. Standards

(Continued on Page 16)

Joint George Mason University and Department of Homeland Security Initiative on Critical Infrastructure Higher Education Programs

The Center for Infrastructure Protection and Homeland Security (CIP/HS) launched a new critical infrastructure and higher education initiative in partnership with the Department of Homeland Security (DHS) Office of Infrastructure Protection.

"The new initiative will create a comprehensive, unified education and training system that produces and sustains the leaders and workforce required to ensure the protection and resilience of the Nation's critical infrastructure," said Mick Kicklighter, CIP/HS Director.

"Protecting and ensuring the resilience of our Nation's critical infrastructure is a top priority for the Department of Homeland Security. It is an important and evolving mission area that is vital in our efforts to preserve our way of life," Todd Keil, Assistant Secretary for the Office of Infrastructure Protection said. "The Critical Infrastructure Higher Education initiative will help to establish the solid academic foundation needed to shape the homeland security workforce for the future."

The Office of Infrastructure Protection — which is funding the higher education initiative — leads the coordinated national program to reduce risks to the Nation's critical infrastructure posed by acts of terrorism and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

"Infrastructure protection professionals must be able to assess risks and vulnerabilities and develop mitigation strategies. They must also be skilled in exercising leadership in crisis situations, enabling them to respond to catastrophes, rapidly restore critical capabilities, and prioritize rebuilding, if required," Keil said. "Courses that address critical infrastructure must be part of a holistic approach to homeland security education."

Many of the disciplines engaged in 'infrastructure protection' such as security, law enforcement or emergency management currently have their own supporting education systems for their respective subject matters. These disciplines are focused on evolving their own education and training programs. "Consequently, most of the focus is targeted to the respective profession in which it occurs, or is delivered within the context of a specific industry sector," Kicklighter said. "There needs to be an ongoing commitment to establish standard educational and training programs and to encourage the adoption and incorporation of these programs within the education systems, and that is exactly what the GMU-DHS partnership initiative does."

The project includes an assessment of existing critical infrastructure degrees, courses, and teaching materials across higher education. The assessment will summarize offerings in higher education, identify best practices, ascertain unmet needs, and offer recommendations for improving infrastructure protection education. CIP/HS will subsequently develop a new higher education curricula focused on infrastructure protection that will serve as a prototype for graduate courses and certificate programs. This curricula could be taught at colleges and universities in their schools of business, public policy, engineering, science, health, government, and other departments.

Potential future activities include development of a certificate program based on the higher education infrastructure protection curricula and modification of an executive master's degree to provide an infrastructure protection concentration.

"Throughout this process, external experts from academia, industry, and government will review, critique, and provide advice on the project from their various perspectives," Kicklighter said. The resulting courses will be non-proprietary and the materials will be made available to any interested university or institution.

(Continued on Page 18)

James Madison University Presidential Remarks

The following remarks were delivered by Linwood H. Rose, President, James Madison University on the occasion of the 5th Annual Spring Symposium, Institute for Infrastructure and Information Analysis (IIIA), National Academies-Washington, DC. May 12, 2010.

General Kicklighter, thank you for being in attendance this evening. Colonel Barlow and Professor Skelley congratulations on your awards presented earlier in the program.

James Madison University (JMU) through the Institute for Infrastructure and Information Assurance developed a unique partnership with the Federal Facilities Council of the National Academies in 2006 to host a series of symposia focused on key issues in national and homeland security.

Past symposia have examined:
- 2006 "Homeland Security: Engaging the Frontlines"
- 2007 "Cascading Infrastructure Failure Avoidance and Response"
- 2008 "Fostering Public-Private Partnerships"
- 2009 "Protection of Large Facility Complexes"

And this year our subject is "Safe, Secure and Sustainable Facilities."

Thank you Ms. Stanley for your work on behalf of the Federal Facilities Council and the National Academies in helping to organize the event and for your commitment to the partnership with JMU.

Mahatma Gandhi said "You must be the change you want to see in the world." At James Madison University we take that to heart. In fact, our theme for the last several years has been *Be The Change*. Our mission is to prepare students to be educated and enlightened citizens who lead meaningful and productive lives. We take the word "citizen" quite seriously in that we expect our students to leave our university with a sense of obligation to serve the communities in which they live and work.

We encourage each student to be a change agent for the public good. We realize that not all will represent the change that they would like to see in the world, but we want to prepare them for that role.

I fear that there are too many of us who wait for the government to tell us what to do. To wear our seat belts, to stop smoking, to eat properly, to control the thermostat and so on. What has happened to self-reliance and personal responsibility, personal initiative and personal action?

On matters of the environment, I am pretty sure that if we wait for governments to tell us what to do we are in deep trouble because political forces will not do what us necessary in the time we have.

And I don't think business can do it, because of the fixation on short-term financial gain. Although I do believe that some businesses are recognizing that long-term viability, and sustained prosperity, depends

Mick Kicklighter, Director of Mason's CIP/HS, and JMU President Linwood Rose. *Photo courtesy of JMU IIIA.*

(Continued on Page 14)

JMU Remarks *(Cont. from 13)*

on socially responsible business decisions.

This requires cultural change and you don't accomplish that through law or directive — it can only come through education. And we had better get busy, because this isn't just about our personal consumption habits, it is about numbers as well. Tom Friedman in *Hot, Flat and Crowded* has pointed out, that part of the issue today, and in the future, is global population growth.[1] Currently, there are 1.3 billion people in China alone. In 2020 there will be 1.5 billion.

If one visits Brazil, China, Indonesia, countries that we used to think of as developing nations, you cannot help but notice that the people of those countries want to live like us. Like Americans — with our conveniences, our technology and our comforts. You cannot blame them. These conveniences, associated with prosperity, devour energy, natural resources, land, and water and emit waste. Friedman claims that the reality is that the planet cannot support a world full of people living like Americans — at least the way we live now.

Each month we are adding 7-8 million people to the planet. A member of our JMU faculty helped me understand the implications of that number. New York City has 8 million residents. The Commonwealth of Virginia has 8 million residents. We are adding the equivalent of the Commonwealth of Virginia, with all of its people, its infrastructure, its consumption and its waste to this planet each month!

We cannot wait for the government to tell us what to do! That is why at JMU we have adopted the initiative "Stewardship of the Natural World." There is nothing really wrong with the term "environmental sustainability," but we wanted to take a more comprehensive view.

JMU President Linwood Rose. *Photo courtesy of JMU IIIA.*

We have joined with other colleges and universities in this effort. As of December 2009, 665 colleges and universities in the 50 states and the District of Columbia had become signatory schools of The American College and University President's Climate Commitment.[2]

These schools represent 5.6 million students — one-third of the higher education population in the United States. As the ACUPCC's latest annual report indicates, "Signatory schools are showing the rest of society how to work quickly toward climate neutrality. They are dramatically reducing operating costs, training clean energy workers, and spurring innovation in energy efficiency, transportation, and renewable power. They are teaching tomorrow's architects, business leaders, policy-makers, engineers, economists, and product designers how to operate society sustainably."

The Hippocratic Oath taken by the medical profession promises at a minimum "to abstain from doing harm." The Boy Scouts of America, teach young men to always leave a camping site better than they found it. The University wishes to model good environmental stewardship behavior and practice so that we might meet the needs of the present without compromising the ability of future generations to meet their own needs. We have adopted what we refer to as a Defining Characteristic for the University: *The University will be an environmentally literate community whose members think critically and act, individually and collectively, as model stewards of the natural world.*

(Continued on Page 17)

[1] Friedman, Thomas L. *Hot Flat and Crowded*, New York: Farrar, Straus and Giroux, 2008.
[2] American College & University President's Climate Commitment, 2009 Annual Report.

SARMA's Fourth Annual
Security Analysis and Risk Management Conference

Tuesday, October 5, 2010 at 8:30 am
to
Thursday, October 7, 2010 at 12:00 pm

"The Road to Resilience: A Risk-Based Approach"

Including presentations and panel discussions on:
Infrastructure Resilience
Community Resilience
Cybersecurity Risk & Resilience
Public Policy for Risk Management & Resilience
Resilience Standards
Risk Methodologies & Practices
...and more

Also join us for SARMA's Annual Awards Reception
Tuesday, October 5, 2010 from 5:00 pm to 7:00 pm

Conference and Reception co-hosted by:

SARMA and the George Mason University School of Law's
Center for Infrastructure Protection and Homeland Security (CIP/HS)

George Mason University - Arlington Campus
Original Building, Room 329
3401 Fairfax Drive
Arlington, VA 22201

For regular updates on keynote speakers, presentations and panels, sponsors, exhibitors and more, please check www.sarma.org.

SARMA
Security Analysis and Risk Management Association

GEORGE MASON UNIVERSITY
Center for Infrastructure Protection and Homeland Security

Resilience Conference *(Cont. from 11)*

change with time, he said, and it is important that Americans be at the table to share their perspectives on effectiveness and utility. Peter Gallant, Chief, Corporate Security, World Bank Group, opened his discussion by talking about how the World Bank is unique in that it does not have to abide by any national or State-level standards. Nevertheless, the World Bank answers to an international board of directors and, like other major organizations, requires a risk management strategy. Although the World Bank previously had a small risk management program, after September 11, it expanded dramatically.

(Left to Right) Marc H. Siegel, Commissioner, Global Standards Initiative at ASIS; Peter Gallant, Chief, Corporate Security, World Bank Group; and Alex McLellan, Principal Analyst at the Homeland Security Studies and Analysis Institute.
Photo courtesy of Liz Salice.

In 2001, the World Bank began an analytical process to start identifying risks and potential methods of mitigation. But implementing the program was difficult because of a concern that the organization would simply react to international events and fail to focus in on its own unique requirements. Instead, the World Bank took a "slow paced approach to building a resilient program based on the criticality of the business needs of the Bank," Mr. Gallant said.

Key to the World Bank's initiative was to first distinguish between critical and non-critical business functions. For instance, the Bank operates major international bond trading and portfolio management programs, many of which implicate international political risk challenges in addition to concerns about physical or cyber destruction or disruption. "We looked at our program from a holistic approach and triaged it down to two business lines that we're looking to support," Mr. Gallant said. The World Bank also decided to de-emphasize physical protection of its facilities in lieu of developing redundancy programs to continue operations in a crisis.

Alex McLellan, Principal Analyst at the Homeland Security Studies and Analysis Institute, began his talk by noting that while there are multiple definitions of resilience that have not yet been resolved, the concept has been around for a long time as "a holistic approach to the management of disruptive events."

Looking at communities in coastal Louisiana, Mr. McLellan noted that while in some parishes no oil from the Deepwater Horizon had reached the shores, the local economy was already reeling because the oil and fishing economies have come to a standstill. Yet these areas typically demonstrate "inherent resilience" in that they are challenged every year by meaningful weather events. Whether they will now demonstrate "adaptive resilience" in the face of this new challenge presents an important topic for further research. ❖

A version of this article appeared in the June issue of The Risk Communicator, SARMA's monthly newsletter.

JMU Remarks *(Cont. from 14)*

Like any other organization, we have a structure to focus our efforts. We have an Institute that reports to the president's office. We have working committees that address the curriculum, research, policies and practices, consumption, waste, and transportation.

Initiatives include Valley 25x'25, Virginia Wind Energy Collaborative, and the Virginia Coastal Energy Research Consortium. JMU is also home to the Alternative Fuel Vehicle Lab that provides opportunities for students to convert and adapt vehicles to operate on renewable fuels. The 25x'25 initiative is federally funded as a regional model with the goal of using twenty-five percent renewable energy sources by 2025.

Environmental stewardship is not one more initiative in a string of initiatives. It is not one more ingredient in our stew pot. Instead it is an approach to life. It is transforming how we live and therefore everything about us is redefined. For example, the university's new vehicles must be hybrid, biodiesel, or electric. Serving trays were eliminated in the dining halls, electronic dashboards showing immediate water and power usage are visible in our buildings. New construction is LEED certified. We just completed a gold LEED dining hall and we are presently planning a residence hall renovation and we are targeting a platinum certification for that project.

A focus on sustainability requires us to innovate and to be resourceful. It drives us to imagine. It leads us to opportunity. We can begin now and it will be fun, or we can wait and then the fun will yield to fear and desperation.

"Authentic" stewardship is about undertaking this because it makes life good — not because it makes us look good.

This whole effort is about what people do, not what people say. I believe if we live in a manner that respects our natural world, and that ensures a high quality of life for future generations, then faculty and staff will be drawn to us, students will select us, and donors will want to support us.

Some have suggested that we use a sustainability commitment to make us distinctive. I want no part of that. In fact, if by being good stewards of the natural world, we differentiate ourselves from others we have a problem of immense proportion, because our action alone is insufficient to right this world.

We must undertake this journey to model the way, to cut a path, to make it easier for others to elect the same course. This is about sharing everything we learn and know. After all, we are educators!

The beauty of discovering fire or the wheel is not in the initial euphoria of discovery, it is in the sharing of these wonders to improve the human condition. So to must it be with building a new way of living as part of nature, rather than aiming to be its master.

We have an opportunity to lead the world in developing laws, policies and actions that can ensure a sustainable planet. But despite our knowledge and our ability to innovate, our political system seems to be in a state of gridlock, unable to cope with grand challenges.

So…we each must be the change we want to see in the world! At JMU we are educating people to do just that. Thank you. ❖

KEPCO *(Cont. from 3)*

develop MS and Doctorate degree programs in nuclear engineering. Beginning in the summer of 2012, some select classes will be held at George Mason's Fairfax Campus. The curriculum will provide special courses on the development of core knowledge of Systems Engineering and on building international human networks. The specific curriculum is currently under development. ❖

For more information about this exciting new program, contact Joan Rothenberg at jrothen2@gmu.edu.

InfraGard *(Cont. from 4)*

and Office of Commonwealth Preparedness with their important missions. ❖

For more on the Virginia Fusion Center please see: http://www.vsp.state.va.us/FusionCenter. For more on the Office of Commonwealth Preparedness and the VCIPRSP please see: http://www.commonwealthpreparedness.virginia.gov.

Cybersecurity *(Cont. from 5)*

emerging threats from sophisticated spear-phishing and social network attacks. The group has also discussed the implications of recent international cybersecurity incidents such as the Google attacks and how to strike the delicate balance between ensuring security while also promoting openness and freedom globally. ❖

Education *(Cont. from 12)*

One of the key objectives of the CIP/HS Education and Training Program is to develop professionals who are equipped with the education and skills to understand the Nation's critical infrastructure protection and resilience missions. The Program fosters the importance of collaborative work among critical infrastructure owners and operators and the public sector. "The critical infrastructure mission demands a professional, highly educated workforce and cadre of leaders at all levels of government and in the private sector. We are looking forward to partnering with GMU in this very exciting higher education initiative," Keil said. ❖

For more information on the DHS Office of Infrastructure Protection: www.dhs.gov/criticalinfrastructure.

Should you have questions or want to participate in this project, please contact Devon Hardy at (703) 993-8591 or dhardy1@gmu.edu.

Information Sharing *(Cont. from 9)*

different approach to the issue, arguing that information-sharing is not a problem/solution issue but a deep-seated cultural one. Back in the mid-1990s, he pointed out, few people in government talked about homeland security on a daily basis. While this has since changed, many old attitudes remain, calling for improved public education about the importance and role of the Nation's homeland security posture. Like many of his colleagues on the day's panels, Mr. Lacombe also emphasized the need for metrics able to gauge success in information-sharing.

Closing out the discussion, Tina Gabbrielli, Director of Risk Management and Analysis at DHS, provided an overview of what DHS has learned about the value of information sharing and risk management and what the Department is doing to achieve both. The recent QHSR emphasized the importance of risk management to inform strategic, policy and budgeting decisions and called for the development of a homeland security national risk assessment. Ms. Gabbrielli discussed what the Department is doing to establish an integrated approach to risk management, including building a common lexicon, developing guidelines, creating risk data information sharing systems, and building partnerships. These efforts are intended to create a shared understanding of homeland security risk and ensure unity of effort across the homeland security enterprise. ❖

A version of this article appeared in the April and May issues of The Risk Communicator, the monthly newsletter of the Security Analysis and Risk Management Association (SARMA).

DHS MS&A *(Cont. from 6)*

Another interesting outcome from the workshop was the attendance of a diverse number of key stakeholders in technology and homeland security. Attendees included representatives from: DHS-S&T, the National Infrastructure Simulation and Analysis Center (NISAC), National Laboratories such as Oak Ridge, Argonne, Los Alamos, Sandia, and Lawrence Livermore, several national and international organizations, universities, government entities such as the DoD Office of Secretary of Defense and the Defense Advanced Research Projects Agency (DARPA), as well as representatives from industry and the private sector.

Outputs from the workshop will include a Final Report of the 2010 workshop and a related Broad Area Announcement (BAA) is expected to follow from DHS S&T. These outputs will help DHS S&T formulate near- and long- term investment decisions as well as research strategy, plans, and objectives for modeling and simulation of the Nation's critical infrastructure and key resources. ❖

The Center for Infrastructure Protection works in conjunction with James Madison Univerity 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 Center is funded by a grant from the National Institute of Standards and Technology (NIST).

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