THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 6 NUMBER 5

NOVEMBER 2007

NETL Project

Publishing
Zeichner Risk Analytics
Contact: CIPP01@gmu.edu
703.993.4840

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

This month's issue of *The CIP Report* highlights research conducted by the CIP Program for the U.S. Department of Energy (DOE) as part of the National Energy Technology Laboratory (NETL) Project, and serves as an update to information provided in the July 2006 issue focused on the Energy Sector. The Energy Sector is one of the 17 designated critical infrastructure and key resource (CI/KR) sectors and encompasses infrastructure supporting many of the essential services on which we continually rely. Without the work of DOE, the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Council (NERC), and others such as the U.S. Department of Homeland Security (DHS), many lights would not go on with a mere flick of a switch.

An overview of recent NETL Project work is provided following an article describing an important research effort reflecting months of staff analysis, the evaluation of 47 State Energy Emergency Response Plans. Research on Energy Sector recovery and reconstruction following the 2005 hurricane season is presented along with a summary of the Commonwealth of Virginia Energy & Sustainability Conference. Additionally, information on DOE's Office of Electricity Delivery and Energy Reliability and FERC's Office of Electric Reliability illustrates federal activities to ensure reliable delivery of electricity throughout the Nation.

The testimony of Sally Katzen, visiting professor of law and a senior consultant to the CIP Program, before two subcommittees of the House Committee on Homeland Security on the importance of cybersecurity and public-private partnerships is also summarized. Lastly, an announcement of *The CIP Report* editorial staff transition is offered.

We are pleased to present our work in the Energy Sector as a sampling of the many research initiatives underway at the CIP Program and greatly appreciate your continued support.

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Critical Infrastructure Protection and the Understated "Partnership" Don't Forget the States

By Michael Ebert, Principal Research Associate, and Maggie Adkins, Law Intern

Policy discussions about critical infrastructure protection (CIP) almost always at some point make reference to the imperative of the "public-private sector partnership." Usually, this imperative is made in the context of a statistic, the origins and accuracy of which are not known, that approximately 80 percent of critical infrastructures and key resources (CI/KR) are owned and operated by the private sector. Further, as expressed in the National Infrastructure Protection Plan (NIPP) and the 17 Sector-Specific Plans (SSPs), the public-private sector partnership – more accurately, a series of partnerships far greater than 17 – is a must because the public sector has, and should have, carefully limited regulatory powers to compel the private sector to "do as we say" with regard to CIP.

Implied if not explicit in partnership discussions is that the "public sector" and the "we" refers to the U.S. Department of Homeland Security (DHS) and the eight federal Sector-Specific Agencies (SSAs) that have shared responsibilities for creating the partnerships and SSPs. Leaving to future articles in *The CIP Report* how well DHS and the SSAs actually collaborate and cooperate with each other as collegial peers (the federal public-public partnerships), not enough attention in Washington, D.C. is given to another and equally important imperative. This imperative is the need for effective and respectful public-public partnerships between DHS and the federal SSAs (on the one hand) and state and local governments (on the other). The states, particularly, are very important actors in protecting the Nation's CI/KR, and our federalist system itself is premised on such public-public compacts.

At a recent congressional hearing (October 2007) on how well the SSPs are comprehensively addressing CIP, Members of Congress and expert witnesses representing the federal government wrestled with actual and perceived gaps in the plans. Some of the wrestling probably would not have been necessary if the public-public partnerships for CIP between federal governments and state governments were better developed, and if the institutions, programs, and plans of the states were better recognized in federal Washington.

These public-public partnerships could be, and should be, better than they are today and, because these critical partnerships ostensibly are "voluntary," it is up to all parties to commit to improvements. But in many cases, the national debate on CIP considers states as an afterthought, if that much. States, on the other hand, may not want the kind of "partnership" that might lead to un-funded or under-funded federal mandates . . . or federal preemption of state authorities and responsibilities.

That is not always the case and, by way of example of a public-public partnership that shows promise, one can look to partnerships the Office of Electricity Delivery and Energy Reliability at the U.S. Department of Energy (OE - DOE) is nurturing with the states to deal with energy emergency planning.

An obscure provision of the "State Energy Efficiency Programs Improvement Act of 1990" (P.L. 101-440) requires states to prepare and submit to the Secretary of DOE "energy emergency planning programs" if a state takes funding from the federal government. These "State Energy Emergency Response Plans" (SEERPs), as they are known today, are in many respects state equivalents of the federal Energy SSP. As such, several of these plans provide pieces, on first glance, that appear to be missing with regard to CIP and cyber-CIP – issues that were of considerable concern during that congressional hearing in October. In 1990, the Congress clearly stated that the Secretary had no authority to dictate planning details to the states; he could review and comment on the plans, but "for informational purposes only." Responding to events such as regional energy crises of the late 1990s, September 11th, and the massive August 2003 blackout, DOE saw SEERPs as a means to better protect and coordinate CIP and cyber-CIP, and saw that these state plans

(Continued on Page 3)

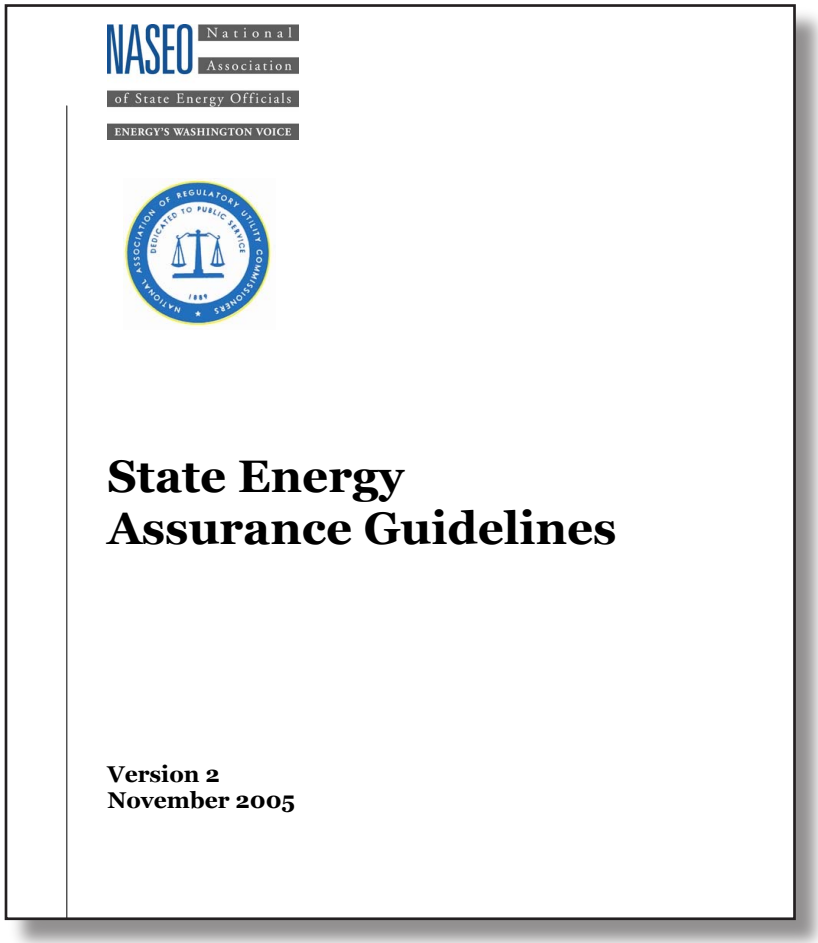
Partnership *(Cont. from 2)*

complemented DOE's SSA activities at the federal level. DOE viewed its limited statutory authority (it could not tell the states to "do as we say") not as an impediment but as an opportunity. OE - DOE worked in collaboration with the states, informally engaging them through established institutions which the states knew and trusted, such as the National Association of State Energy Officials (NASEO) and the National Association of Regulatory Utility Commissioners (NARUC). One result: this informal, voluntary public-public partnership produced highly detailed NASEO "guidelines," published in November 2005, which the states could draw upon to develop better and more comprehensive energy emergency plans. OE - DOE offered its state partners more than funding assistance; it used its convening powers to bring state officials and institutions together, and it offered the expertise and experience of the Department's resources.

When the CIP Program evaluated 47 of these SEERPs for DOE a few months ago, it was clear to us that while there are many factors that determine the "goodness" of a SEERP, states that received assistance from DOE tended to have better plans than those that did not. Plans developed after NASEO published its voluntary guidelines are, overall, better than SEERPs drafted before. And, by the way, CIP Program SEERP evaluations generally track similar findings by the U.S. Government Accountability Office (GAO) when it reviewed federal SSPs: cyber-CIP is an area in need of improvement.

Good public-public partnerships can produce valuable CIP awareness and progress, as the example above illustrates. We look forward to discussing other examples in future issues of *The CIP Report* and urge our readers to suggest where other such partnerships might exist. ❖

When the CIP Program evaluated 47 state/territory "energy emergency response plans" during the summer of 2007, numerical values were established for major plan benchmarks and other criteria based upon voluntary guidelines which were produced as a result of the OE – DOE "public–public" partnerships with the states. For the most part, the partnerships worked through two national organizations, NASEO and NARUC. NASEO and NARUC are, by constitution and membership, entities that state officials "own and control," with OE – DOE participating only as an informal observer. When the evaluations were finished, researchers conducted an analysis of the results, which was subsequently presented to DOE.



The National Energy Technology Laboratory (NETL): An Update on Recent Work

In August 2004, the CIP Program began research with the Department of Energy's National Energy Technology Laboratory (NETL). The research has focused on *Energy and Measures for Risk Mitigation and Transfer.* As the CIP Program's research has continued with NETL, it has brought forth more interesting work and, most recently, has involved projects such as the following:

Critical Electric Power Infrastructure Recovery and Reconstruction

CIP Program researchers examined how certain Gulf Coast states – Florida, Louisiana, Mississippi and Texas – and the federal government responded to the unprecedented energy infrastructure destruction inflicted by Hurricanes Katrina, Rita and Wilma. On October 31, 2006, CIP Program researchers presented an overview of their findings to DOE and experts the Department invited from outside the agency, entitled: *Critical Electric Power Infrastructure Recovery and Reconstruction: New Policy Initiatives in Four Gulf Coast States After 2005's Catastrophic Hurricanes*.

This project provided a stepping stone for the research and presentation that was briefed at the more recent **Commonwealth of Virginia Energy & Sustainability (COVES) Conference**. For further information on this conference, please see the article on page 6.

Another project that came out of NETL this year involved reviewing **State Energy Emergency Response Plans** for 47 different states and territories.

Since 1990, states have a basic, conditional requirement under federal law to develop such "contingency plans" in order to provide more effective state and regional coordination to energy shortfalls and emergencies, and to provide the Secretary of Energy with an awareness of the states' plans, responses and legal authorities. The 47 plans were evaluated against the National Association of State Energy Officials (NASEO) State Energy Assurance Guidelines, Version 2 (November 2005). Through a thorough examination of the NASEO Guidelines, CIP Program researchers developed a set of topical metrics and supporting submetrics. These indicators were organized into a data matrix, which formed the quantitative underpinnings of the evaluations. . . . After concluding the evaluations in August, CIP Program researchers prepared a report which included statistical analyses including visuals (maps, graphs, box plots, frequencies, etc.). The draft report was presented to DOE's Office of

Electricity Delivery and Energy Reliability on September 17, 2007. Subsequent to OE's review of the draft, selected research results may be available on our website.

For more information on the NETL project and detailed overviews of the CIP Program's many endeavors, please visit our website at http://cipp.gmu.edu/; visit the Selective Reports on Critical Infrastructure Recovery and Restoration webpage for additional information on topics explored under NETL. ❖

Supporting Energy Infrastructure: DOE's Office of Electricity Delivery and Energy Reliability

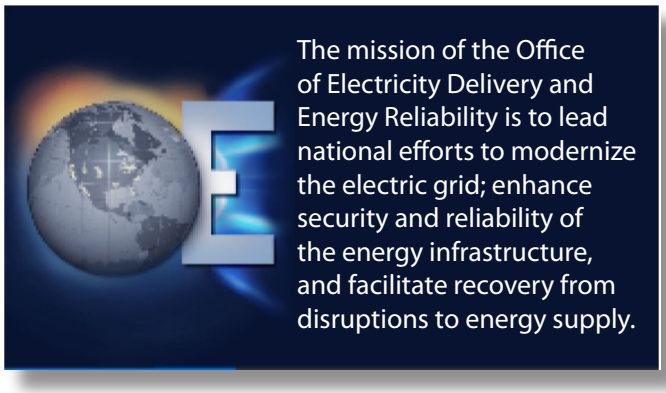
DOE's Office of Electricity Delivery and Energy Reliability (OE) was established in 2005 with the merging of the Office of Electric Transmission and Distribution and the Office of Energy Assurance. OE is responsible for preparedness and response relative to energy emergencies caused by all hazards, as well as recovery efforts in coordination with Energy Sector partners. In addition, it seeks to advance technologies for the modernization and assurance of the Nation's electricity delivery system.

OE is organized into three divisions: Infrastructure Security and Energy Restoration; Research and Development; and Permitting, Siting, and Analysis. OE also operates a National Energy Technology Laboratory (NETL) Site Office that supports infrastructure protection and emergency response through the provision of valuable technical expertise.

Infrastructure Security and Energy Restoration

The Infrastructure Security and Energy Restoration Division coordinates the Department's response to energy emergencies and supports the recovery efforts of State, local, and private sector partners. It also manages a national critical infrastructure protection program, working with the U.S. Department of Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), and other agencies as appropriate.

To assist in enhancing infrastructure security, the Division analyzes energy infrastructure vulnerabilities and offers information on protective measures. Furthermore, it supports Emergency Support Function (ESF)-12 (Energy) operations as outlined in the National Response Plan.



Research and Development

The Research and Development (R&D) Division manages projects to advance technologies supporting electric delivery and infrastructure security. Specifically, according to the OE website, it will "[p]lan, implement, and evaluate a portfolio of electric delivery and infrastructure security technology projects, visions, R&D roadmaps, public-private partnerships, technology transfer and commercialization plans, and education and outreach strategies." The Division also is responsible for developing, implementing, and maintaining a cyber security program.

Permitting, Siting, and Analysis

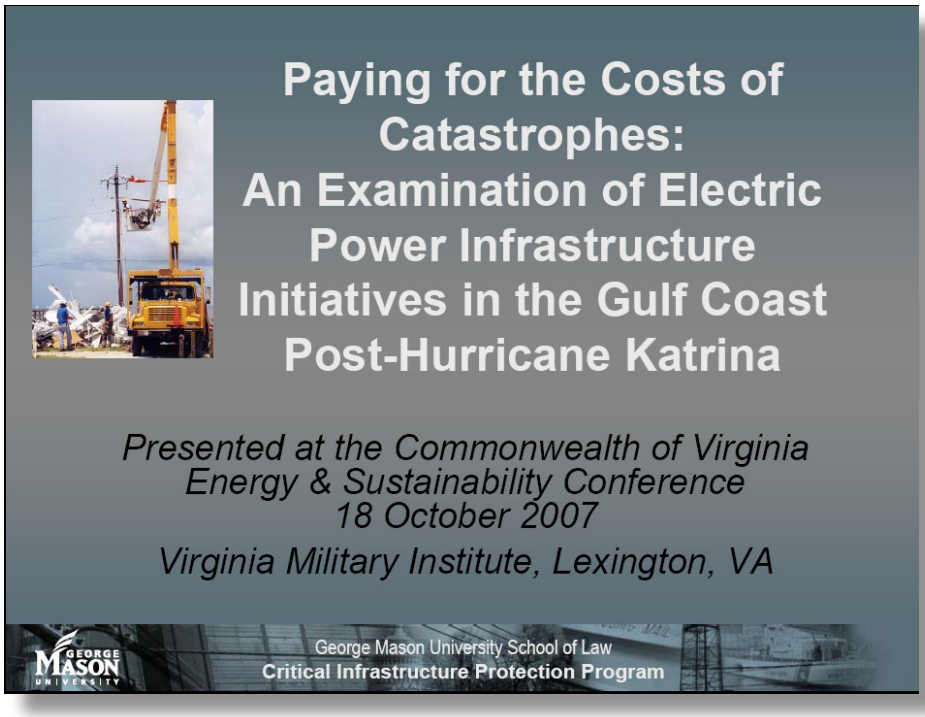
The Permitting, Siting, and Analysis Division analyzes factors that can negatively impact the operation of electric transmission and distribution systems. Such factors include physical, regulatory, and institutional issues and other limitations or "bottlenecks" facing electric delivery. In addition to this analysis, it works with organizations on various levels to "develop effective solutions and assess alternatives increasing the reliability and efficiency of electric market operations." The Division also coordinates with DOE's four power marketing administrations (Bonneville Power Administration, Southeastern Power Administration, Southwestern Power Administration, and Western Area Power Administration), who ensure broad use of electricity at low consumer rates.

The Division authorizes applications for international electric transmission facilities and for the export of electricity generated in the United States, and regularly reviews data on the U.S. international electricity trade. It also participates in discussions with Canada and Mexico regarding electricity trade and regulation.

Additional information on OE can be found at: http://www.oe.energy.gov/. ❖

Paying for the Costs of Catastrophes

By Christine Pommerening, Ph.D., Senior Research Associate



Not many conferences have a mission statement, but the one formulated by the organizers of the second annual Commonwealth of Virginia Energy & Sustainability (COVES) Conference, held at the Virginia Military Institute in October, certainly captures the unique role of states in shaping energy policy: "The mission is to help Virginia position itself so that businesses, governments, and citizens anticipate the energy challenges ahead and make wise decisions for a bright future. States serve our nation best when we are laboratories for developing innovative and effective solutions." (See http://www.covesva.org/Program/2006/mission.htm). It turns out that innovative and effective solutions are not limited to supply and demand – states are also innovators when it comes to developing new instruments for financing and recovering costs associated with providing electricity to their citizens. The CIP Program was invited to present some of its research in this area at a panel that addressed the cyber and homeland security challenges of electricity transmission. Under the title "Paying for the Costs of Catastrophes: An Examination of Electric Power Infrastructure Initiatives in the Gulf Coast Post-Hurricane Katrina" (see http://www.covesva.org/Program/PDF/cost-recovery_GMU_CP.pdf), we reported selected findings from a DOE-sponsored study on "Critical Electric Power Infrastructure Recovery and Reconstruction." In this study, we evaluated cost recovery innovations developed by a number of states that were hit hard by hurricanes during the 2004 and 2005 hurricane seasons. In particular, we examined the emergence of a specific type of asset-backed security known as 'storm bond,' and the usage of federal funding through so-called Community Development Block Grants. Both instruments are not uncontroversial.

Securitization via storm bonds proved to be difficult to administer for even the most experienced public utilities – the process of defining the terms and conditions, setting up special issuing entities, finding underwriters, and negotiating with institutional investors is time-consuming and costly. The federal grant process was also beset with problems – unclear timelines and appropriations, the involvement of multiple agencies outside of energy administration, and the need for multiple certification caused long delays. In addition, more fundamental question of equitable distribution of costs and benefits arise – between states and the federal government, utility shareholders and ratepayers, Wall Street investors and taxpayers.

Given that there is no optimal solution, the four states examined in the study have all taken rather different approaches, as laid out in the report (see http://cipp.gmu.edu/projects/DoE-NETL-2006.php). Thus, decision-makers in Virginia, when faced with similar issues, will have to charter their own course as well. ❖

New Federal Energy Regulatory Commission Office Will Enhance Efforts to Assure Electric Reliability

The Federal Energy Regulatory Commission (FERC) is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil throughout the United States. On September 20, 2007, FERC announced the creation of a new office focused on the reliability of the Nation's electric infrastructure, the Office of Electric Reliability (OER). Specifically, OER oversees the development and review of mandatory reliability and security standards and ensures compliance with approved mandatory standards by owners/operators and users of the U.S. bulk power system.

- Participation in the standards development process with NERC to enhance the quality of proposed reliability standards;
- Review of reliability programs for effectiveness and standards compliance;
- Assistance with analysis and investigations of concerns with the bulk power system with regard to reliability standards compliance and standards effectiveness;
- Oversight of NERC's resource adequacy assessments for potential concerns with efficient operability of the bulk power system;

"Mandatory and enforceable reliability standards and a strong reliability regime are critical elements of the Commission's new regulatory authority over the reliability of the nation's bulk power system, which Congress enacted in the Energy Policy Act of 2005. Today's announcement appropriately raises the profile of this important effort." - FERC Chairman Joseph T. Kelliher

Previously a component of FERC's Office of Energy Markets and Reliability, now renamed the Office of Energy Market Regulation, OER helps process reliability-related filings with FERC and review assessments of the bulk power system conducted by the North American Electric Reliability Council (NERC), the certified electric reliability organization (ERO) for the United States. It also identifies potential concerns in regulatory or congressional language affecting the Nation's electric infrastructure.

In addition to those activities outlined above, OER's responsibilities include:

- Participation in regional project planning processes to ensure adequate consideration of reliability requirements;
- Working with energy stakeholders to promote energy reliability and security, including:
  - Federal agencies and other government entities, such as state-level regulators
  - National Association of Regulatory Utility Commissioners
  - ERO and Regional Entities (REs)
  - Regional Transmission Organizations (RTOs)/ Independent System Operators (ISOs)
  - Owners/operators of the bulk power system
  - Users of the bulk power system
  - Customers
- Monitoring of events impacting the bulk power system and maintaining an emergency reporting system for the relay of pertinent information to FERC leadership;
- In cooperation with stakeholders, assessment of factors with potential negative impacts on the bulk power system and cost recovery options to address such factors, as well as any localized constrained areas; and
- Development of procedures and standards for the security of the bulk power system.

Additional information on OER can be found at: http://www.ferc.gov/about/offices/oer.asp. FERC's announcement of this new office can be found at: http://www.ferc.gov/news/news-releases/2007/2007-3/09-20-07-E-1.asp. ❖

CIP Program Testimony Focuses on Incentives to Improve Cyber-CIP

By Maggie Adkins, Law Intern

On October 31, 2007, Sally Katzen, visiting professor of law at the George Mason University School of Law and a senior consultant to the CIP Program, testified before the House Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology and the Subcommittee on Transportation Security and Infrastructure Protection in a hearing titled "Enhancing and Implementing the Cybersecurity Elements of the Sector Specific Plans." The formal testimony developed by Professor Katzen was based on written testimony produced through a collaborative effort between Professor Katzen; two senior CIP Program research staff members, Michael Ebert and Dr. Christine Pommerening; and legal intern Maggie Adkins.

The focus of Professor Katzen's testimony was how to improve cybersecurity elements in the SSPs. Professor Katzen and the CIP Program researchers stated they are convinced that the key to the cybersecurity dilemma is integrating standards into Enterprise Risk Management (ERM) principles and techniques, for which the researchers suggest a definition:

ERM is the systematic application of strategic and operational management policies, procedures and practices aimed at identifying, analyzing, evaluating, treating, and monitoring all risks to the business processes of an enterprise.

The emphasis is on the enterprise as a whole. Professor Katzen testified that researchers found ERM particularly attractive because ERM shines a light on cyber-CIP risks and all other enterprise risks at very high levels of accountability in the corporation, including the boardroom. The benefits of ERM are not limited, of course, to the private sector; governments, most notably municipalities, are looking to ERM as a valuable tool. While ERM has benefits beyond cyber-CIP, also this integrated, enterprise-level approach to the identification, assessment, and mitigation of all risks has particular merit in addressing cyber risks that permeate an organization's many internal and external relationships.

"The Sector Specific Plans were written . . . with critical inputs and expertise from the private sector, and are necessarily only as good as the levels of collaboration and trust that went into them. And how good are they? According to the U.S. Government Accountability Office as well as other experts, these plans fall short . . . including but not limited to cybersecurity. We have a long way to go."

The testimony addressed a recent GAO report that found that the majority of SSPs have no established way of setting meaningful benchmarks and measuring progress. Benchmarks and measurements are of extreme importance when safety as well as time and money are on the line. The testimony suggested that the Paperwork Reduction Act (PRA) is not an impediment to enhancing and implementing the SSPs, but instead assures the quality of statistics that might be sought by DHS while acting as a tool that reduces the burdens government regulations tend to place on the private sector, and so could in fact be useful to measuring the progress of the SSPs.

Though Professor Katzen's testimony highlighted the benefits of ERM to cyber-CIP, the testimony was mainly focused on how the government can incentivize the Sector-Specific Agencies (SSAs) responsible for the 17 CI/KR sectors to improve their cybersecurity elements. Professor Katzen did not urge new government regulations but instead suggested the use of market-based incentives. Professor Katzen's recommendations were for the government to sponsor "ERM for CIP" workshops; provide tax credit to companies that are ERM certified; establish a public recognition and reward program for companies that raise the bar on cyber-CIP; provide preference in federal government contracting to companies that are cyber-secure and to lead by example.

(Continued on Page 9)

Testimony *(Cont. from 8)*

Professor Katzen primarily discussed the importance of the federal government leading by example in cybersecurity issues, because the role of state and local governments in critical infrastructure protection often is unfortunately overlooked. True partnerships based on respect and voluntariness between the public-public and public-private sectors can be cultivated by the federal government. Professor Katzen used the recent example of the good public-public partnership between DOE and the states as a possible model for how DHS should proceed in its efforts to help improve the cybersecurity elements of the SSPs. Professor Katzen stated that though DOE has rather limited power in examining "State Energy Emergency Response Plans" (SEERPs), it is still able to help the states to improve their plans. By design, SEERPs should contain components to include emergency planning, coordination, response, and cyber-CIP.

CIP Program researchers evaluated 47 plans against a series of metrics which were developed with the assistance of OE-DOE and others. Of importance to DHS and related to the importance of effective federal-state partnerships, CIP Program researchers did see some positive correlation between analysis results and whether states received assistance from DOE. Professor Katzen's testimony also used her previous experience to discuss the importance of leading by example: "[O]ne proven way to incentivize is to lead by example. Every successful coach, teacher, executive, or parent knows this, and it was one of the most important lessons I took from my experience at OMB during Y2K. A potent incentive for the private sector is for the public sector to clean up its act and protect the people's CI/KR – first. . . . Another very important lesson we learned from Y2K is the importance of collaborative, collegial, and effective public-public partnerships – that is, the incredible value of respectful federal-state-local government partnerships."

"The states are vital partners in critical infrastructure protection. Traditionally, state (and often local) governments have been at the front line of awareness, preparedness and response. . . . Whether such relationships can survive where there are fears of impending federal preemption is an open question."

Professor Katzen's testimony urged DHS not to seek out more command and control powers but instead to adroitly use its convening powers, take full advantage of its collaborative opportunities, and work collegially through problems with those federal and state agencies that have not only the expertise but also the experience and relationships with their private sector counterparts in the various CI/KR sectors. Similarly to DOE, DHS, within its current framework, has the opportunity to improve cybersecurity in SSPs, if it uses appropriate incentives.

Other organizations and government officials that testified at the hearing included Greg Garcia, Assistant Secretary of the Office of Cybersecurity and Communications of DHS; David Powner, Director of the Information Technology Management Issues with GAO; and J. Michael Hickey, Chairman of the Communications Sector Coordinating Council. All of the testimony is available online at http://hsc-democrats.house.gov/hearings/index.asp?ID=100. For a summary of the recommendations presented by professor Katzen during her testimony, please see page 10. ❖

"For DHS to successfully navigate these waters requires an almost unprecedented level of constructive interplay between and among many federal and state agencies. For the most part, DHS has few authorities to force its federal or state partners or the private sector owner/operators of CI/KR to 'do as we say.'"

Cyber-CIP Recommendations in a Nutshell

- Sponsor "ERM for CIP" workshops – DHS as well as the non-DHS SSAs should partner with established and recognized providers of ERM education, training, and certification to develop a workshop (or series of workshops) that would be offered to qualifying private-sector owner/operators of CI/KR.

- Alternatively, provide a tax credit to qualifying companies that obtain education, training, and credentialing in ERM for CIP.

- Establish a public recognition and rewards program for companies that have raised the bar on cyber-CIP. A useful analogy is the Energy Star program, which recognizes companies that produce energy-efficient products. To receive what we might call Cyber Star recognition and rewards, qualifying criteria should be measurable and raise the bar over time.

- Provide preferences in federal government contracting for companies that own/operate CI/KR and have obtained training and certification in "ERM for CIP" and/or received the recognition/reward. Preferences should be sunsetted to incentivize continual improvement and continued education and training.

- Governments must lead by example. Governments – federal, state, and local – must be models of enhanced cyber-CIP if for no other reason than that failing to adequately protect 20 percent of critical infrastructures that governments own/operate for the American people is not acceptable. But there is another reason: one proven way to incentivize is to lead by example. Every successful coach, teacher, executive, or parent knows this. A potent incentive for the private sector is for the public sector to clean up its act and protect the people's CI/KR – first.

The CIP Report Editorial Staff

The composition of the editorial staff of *The CIP Report* has recently transitioned. The monthly newsletter now features three new editors: Colin Clay, Elizabeth Jackson, and Olivia Pacheco.

Colin Clay recently joined Zeichner Risk Analytics (ZRA) as a Senior Program Analyst after several years in the nonprofit field. He serves as the editor of ZRA's regular publications, including *The CIP Report.*

Elizabeth Jackson has written numerous pieces for *The CIP Report* and was most recently listed as a Staff Writer. Liz performs special projects on a range of issues, including the history of CIP in the United States, international CIP policy and planning, risk management, and the composition of CI/KR sectors.

Olivia Pacheco was previously working with the Private Sector Program and transitioned to the CIP Program's core research team at the beginning of this year. She assisted the Director with special projects and provides support for several research efforts, both internal and external.

Colin, Liz, and Olivia are pleased to join the editorial staff of *The CIP Report* and look forward to continually enhancing this valuable newsletter.

***

Jeanne Geers has resigned from her position at ZRA, where she served for five years as an editor of *The CIP Report.* She is taking a career hiatus to accompany her husband and three daughters to Tallinn, Estonia, where he is posted to the NATO Centre of Excellence on Cooperative Cyber Defence.

After serving as Associate Director and editor of *The CIP Report* for over three years, Jessica Milloy Goobic has resigned from the CIP Program. Jessica leaves to join a strategic consulting firm specializing in human capital management located in Alexandria, Virginia.

Jeanne and Jessica greatly enjoyed their tenures as editors of *The CIP Report* and wish the new editorial staff the best of luck.

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

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

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