The CIP Report

VOLUME 1, ISSUE 6

DECEMBER 2002

Electricity Sector Issue

CIP Project Staff

John McCarthy
Executive Director

Emily Frye
Associate Director, Legal Programs

Kevin “Kip” Thomas
Associate Director,
Research Programs/
Research Associate Professor

Meredith Gilchrest
CIP Law and Policy Research Archivist/
Outreach Program Manager

Rebecca Luria
CIP Project Administrator /
Executive Assistant

George Baker
Interim Director
JMU Institute for Infrastructure and Information Assurance

Ken Newbold
JMU Outreach Coordinator /
JMU CIP Project Liaison

Contact: cipp01@gmu.edu
703-993-4840

This issue of *The CIP Report* focuses on the Electricity Sector. The amount of change in this sector during the past several years is staggering. Industrial and commercial customers, trying to sustain competitiveness in a global market place, are pressuring suppliers of electricity to reduce prices; at the same time, the demand for and use of electricity has grown to support more sophisticated service delivery and manufacturing processes at higher speed and accuracy.

Congress, the Administration, and relevant stakeholder communities are working closely to discuss standard market design (SMD) proposals – and this dialogue will profoundly impact multiple critical infrastructure issues and challenges. Participation in wholesale activity will require an appropriate level of security, which includes a cyber-security component to support transmission integrity across the grid.

The Electricity Sector has taken very seriously the responsibility of protecting systems and providing reliable service delivery. The North American Electric Reliability Council (NERC), designated by Presidential Decision Directive 63 as the Sector Coordinator, has worked closely with its designated Sector Liaison, the Department of Energy, and with the Federal Energy Regulatory Commission (FERC), the National Infrastructure Protection Center (NIPC), and a broad spectrum of other organizations to develop security-related programs. NERC has outlined, developed, and disseminated complex critical infrastructure policy materials – covering threat and vulnerability assessments, information sharing analysis, and indications & warning. This issue provides information on NERC’s Critical Infrastructure Protection Advisory Group. Readers will benefit from reviewing an impressive portfolio of accomplishments.

THE TECH CENTER
National Center for Technology & Law
CRITICAL INFRASTRUCTURE PROTECTION PROJECT

Similarly, government agencies, especially the FERC, the National Infrastructure Simulation and Analysis Center, the Office of Energy Assurance at the Department of Energy, and the NIPC have developed important critical infrastructure initiatives focused specifically on electric power. We include many of these programs in this issue to highlight achievements as well as models for other infrastructure sectors. ◆

Discussion with Alison Silverstein – Special Advisor to the Chair of the FERC

The Federal Energy Regulatory Commission (FERC) has become one of the most dynamic Federal government agencies in promoting national critical infrastructure goals. In a discussion with the GMU CIP Project, Alison Silverstein, Special Advisor to the Chair of the FERC, outlined the agency's operating philosophy as well as programmatic accomplishments since she signed on just one week after the 9/11 attacks. The following four activities are part of the strategic programs and accomplishments developed by the FERC in the aftermath of the 9/11 attacks.

- **Facilitating Security Cost Recovery – Safeguarding our Energy Infrastructure**

Cost recovery in the electric power sector has always been a critical concern. This is especially so with regard to capital investments in the areas of security and infrastructure reliability. In order to address these concerns, the FERC has established a cost recovery program for security-related investments. On September 14, 2001, the FERC issued its *Statement of Policy on Extraordinary Expenditures Necessary to Safeguard National Energy Supplies*. This policy offers assurances that the FERC will approve applications to recover "prudently incurred costs necessary to further safeguard the reliability and security of our energy supply infrastructure in response to the heightened state of alert."

- **Accessing Critical Energy Infrastructure Information: Balancing Freedom of Information with Critical Infrastructure and Security Concerns**

The FERC has developed one of the most progressive public access and freedom of information policies and programs since the 9/11 attacks. First, the FERC immediately removed from *easy* public access certain documents; FERC changed its policy in order to restrict general and unfettered public access to certain sensitive information – such as detailed infrastructure maps – that could undermine protection of the nation's energy infrastructure.

Working through the Federal Register process, the FERC defined Critical Energy Infrastructure Information (CEII) as information already exempt under the FOIA and is in the process of finalizing regulations to balance open access with greater protection of CEII information. These FERC policies and rules are being examined by other Federal agencies as a model for open access to sensitive infrastructure information.

- **Collaboration with NERC on Cyber Security- Enhancing Transmission Integrity**

The FERC-lead process of defining a Standard Market Design includes cyber security standards developed by the

continued on page 8►

Alison Silverstein Special Advisor to the Chair

Secret to Success at the FERC in CIP activities:

"Highly focused, strategic, performance and results oriented – and the best and the brightest people."

Education

MBA	Stanford University
MSE	Systems Analysis and Economics The John Hopkins University
BA	Economics The Johns Hopkins University

Activities Undertaken by the Electricity Sector to Address Physical and Cyber Security

The North American Electric Reliability Council (NERC) is a not-for-profit organization formed after the Northeast Blackout in 1965 to promote the reliability of the bulk electric systems that serve North America. NERC comprises ten Regional Reliability Councils that account for virtually all of the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. In addition to its job of "keeping the lights on," NERC serves as the electric industry's contact and coordinator in the United States and Canada for bulk electric system security matters and operates the Electricity Sector's Information Sharing and Analysis Center (*see page 7*).

Lou Leffler is the Manager-Critical Infrastructure Protection for NERC, and has the responsibility to facilitate the work of NERC's Critical Infrastructure Protection Advisory Group. Mr. Leffler is a member of the ES-ISAC team, and is the Sector Coordinator.

Critical Infrastructure Protection Advisory Group

Following issuance of the President's Commission on Critical Infrastructure Protection Report in 1997 and the President's Decision Directive 63 in 1998, the Secretary of the U.S. Department of Energy requested NERC to accept the role as Electricity Sector Coordinator for Critical Infrastructure Protection. NERC President and CEO, Michehl Gent, with approval of the Board of Trustees, accepted this assignment as a logical extension of NERC's mission. NERC established a study and action group--which is now the Electricity Sector Critical Infrastructure Protection Advisory Group (CIPAG) with a direct reporting relationship to the NERC Board. Essential to progress in efforts to enhance security of the Electricity Sector is the cooperation of all segments within the Sector. The CIPAG brings together the generation and transmission providers, public and investor-owned utilities, power marketers, regional transmission organizations and independent system operators, electric power associations, and government agencies. Both Canadian and United States entities participate.

Indications, Analysis, and Warning Program

After the CIPAG established its relationship with the Sector Liaison, the U.S. Department of Energy (DOE), the advisory group and representatives of the DOE met with the National Infrastructure Protection Center (NIPC). From this has emerged a close security working relationship that resulted in the development of the Electricity Sector – NIPC Indications, Analysis, and Warning Program (IAW Program).

The IAW Program provides several reporting mechanisms to enable reliable and secure communications between Electricity Sector entities and the NIPC. The IAW Program Standard Operating Procedures (SOP) contains event criteria and thresholds with report timing for nine physical/operational and six cyber/social engineering "event types." Those events to be reported include those occurrences to an Electricity Sector entity that are either of known malicious intent or are of unknown origin. Events include

continued on page 4►

Micheh R. Gent
President and CEO
NERC

NERC, continued from page 3

such things as the loss of a key element of an electric power system or telecommunications critical to system operations, announced threats, intelligence gathering (surveillance), computer system intrusion (each event type contains specificity as to level of actual or potential impact on operations of the reporting electric entity). Note that electric "entities" include generation, transmission, distribution, overall system reliability coordination, and power marketing.

The power of the IAW Program lies in the fusion of incident information from many sources (government and private sectors) in one place for continuous analysis and prompt dissemination of threat and possible vulnerability information back to the sectors. The IAW Program was approved for voluntary use by the Electricity Sector in July 2000. Over the next several months, NERC and NIPC conducted three workshops designed to raise the Sector's awareness to the security issues and to introduce the IAW Program. The program is in use currently.

From the Indications, Analysis, and Warning Program:

This SOP (Standard Operating Procedure) establishes voluntary procedures for implementing the information reporting, analysis and warning provisions of the National Infrastructure Protection Center's (NIPC) national level Indications, Analysis & Warning program for electric power. This program has been established to enable the NIPC to provide timely, accurate, and actionable warning for both operational and cyber threats or attacks on the national electric power infrastructure.

Other Security-Related Activities

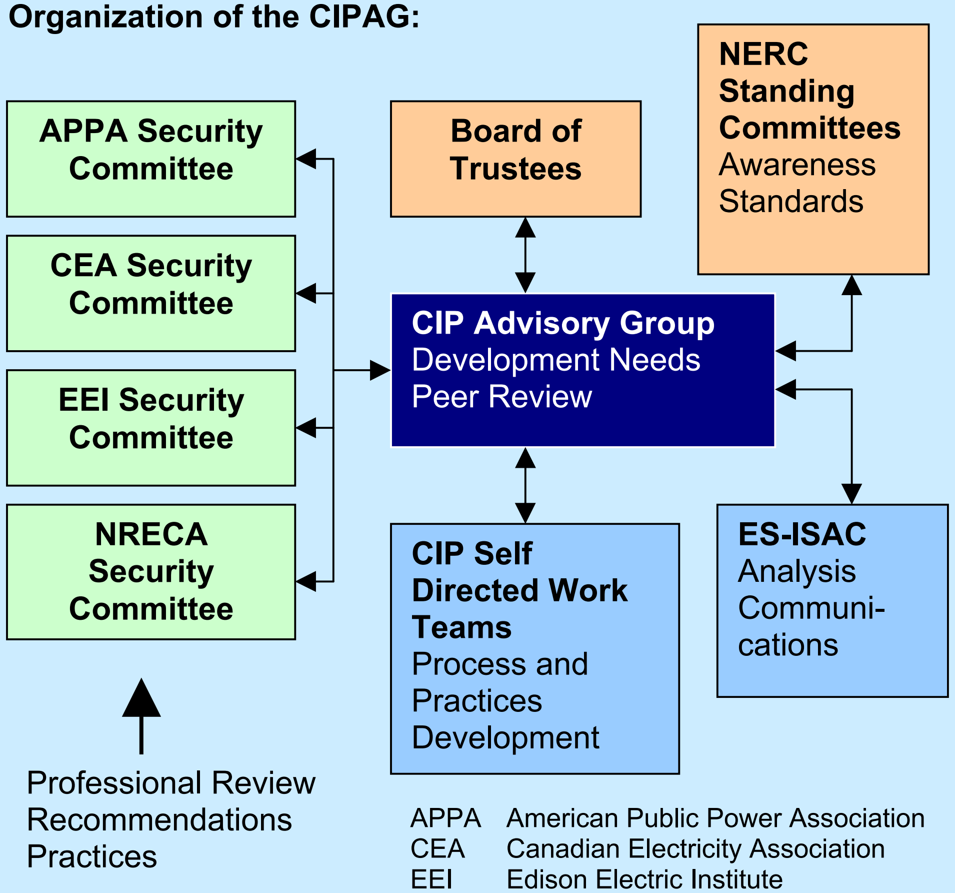
Following are other activities undertaken by NERC:

- Published an Approach to Action for the Electricity Sector
- Published Security Cases for Action for the Electricity Sector
- Developed and maintains set of Security Guidelines
- Developed a Threat Alert System for the Electricity Sector that coordinates with the Homeland Security Advisory System (HSAS)

The above documents are available via the NERC and ES-ISAC Internet sites:
http://www.nerc.com
http://www.esisac.com

The electric industry operates in a constant state of preparedness. Planning, training, and operating synchronous grids prepares the electric industry for natural disasters such as earthquakes, floods, tornadoes, energy emergencies and attacks of sabotage or terrorism. NERC has elevated critical infrastructure protection to be the focus of a high-level advisory group comprised of all ownership segments in the electric industry. ◆

Organization of the CIPAG:



APPA	American Public Power Association
CEA	Canadian Electricity Association
EEI	Edison Electric Institute
NRECA	National Rural Electric Cooperative Association

Supervisory Control and Data Acquisition (SCADA) Systems

Dr. George Baker and Mr. Allan Berg

Dr. George Baker

Our critical national infrastructure systems have become almost universally dependent upon computer-based control systems technically referred to as supervisory control and data acquisition (or SCADA) systems. SCADA systems evolved from the telemetry and event-alarm systems developed in the early days of utilities. They have three major components:

1. Remote sensors and control devices (referred to as remote terminal units or RTUs) which acquire data and respond to operator commands

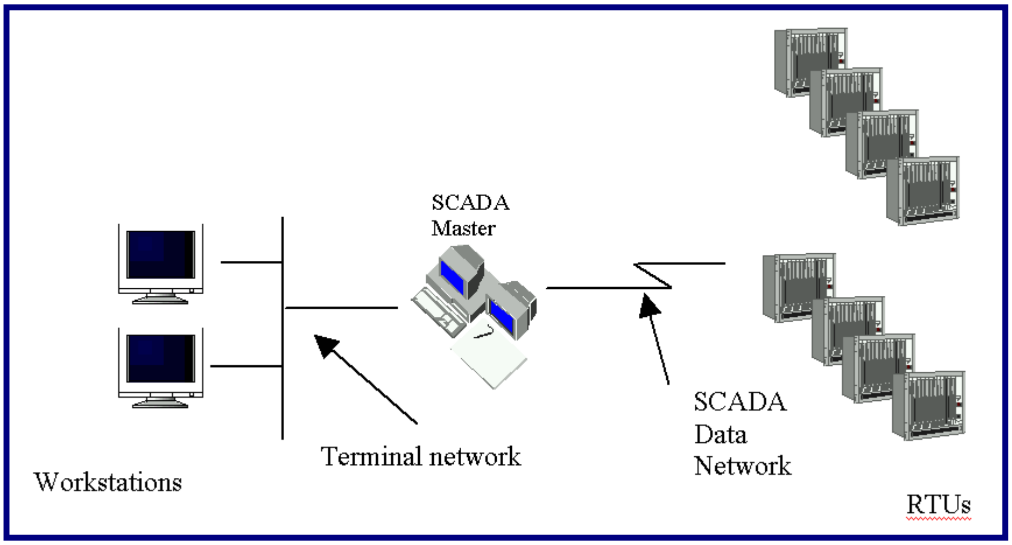
2. Supporting two-way communication system links to transmit the data via telephone, microwave, cable, or satellite circuits between the master control station and the RTUs

3. Master control stations where sensor information is stored in memory and displayed on central computer screens enabling operators to track the system status/problems. SCADA enables remote control of system operation either automatically or initiated by operator commands.

Infrastructures that are heavily dependent on SCADA include electric power generation and distribution, water distribution, oil and gas pipelines, telecommunications, railroads, and food processing. SCADA is employed worldwide and often crosses national boundaries. As an example, pipeline companies use SCADA to monitor and control the flow of billions of cubic feet of natural gas every day. RTUs along the pipelines measure and transmit data on pipeline pressure, flow rates and the open/closed state of flow-controlling switches and valves. The master control station operator interfaces incorporate sophisticated software used by operators to instantaneously view the status of pipeline operation and enables them to open and close valves to control gas flow hundreds of miles away.

With the widespread use of SCADA systems, computers have become the “basis element” for much of our critical infrastructure. As a consequence, the disruption of controlling computer terminals and networks due to natural disasters, electric power failure, accidents, or hostile activity can have catastrophic consequences. Hostile activity is of highest concern. Because of computer control, critical infrastructure services can be disrupted remotely -- common hacker tactics can be used to destroy real-world lives and property. Attackers may insert malicious code, such as viruses, Trojan Horses, and/or logic bombs to destroy databases required for SCADA management of communications systems or industrial process systems involved in distributing electricity, fuel, or water. Attackers can also break into SCADA systems and take over real-time control of critical processes. In a recent incident, hackers were able to open and close the flood gates of a

continued on page 6►



SCADA, continued from page 5

Mr. Allan Berg

hydroelectric dam by breaking into the resident SCADA system. It is conceivable that similar attacks could occur on electric generation and distribution systems and the public switched network. Information on SCADA systems and how to program them turned up on al Qaeda computers seized this year.[1]

Physical attacks on SCADA systems can also have serious consequences. Physical destruction of control facilities and cutting the lines of communication by severing cables or jamming microwave links are possible means of attack. One problematic aspect of SCADA systems is that when they fail, in many cases the controlled process continues to execute the last command before failure. Thus open valves stay open and running motors continue to run with potentially catastrophic consequences. An attack on an Australian water treatment SCADA in 2000 resulted in sewage overflows into a public water system. In Washington State, authorities cited improper SCADA performance as a contributing factor in a 1999 gasoline pipeline rupture and fire that killed three.

SCADA system protection poses many challenges. SCADA systems are very different among and within critical infrastructure systems--one protection technique does not fit all. Deregulation has militated against protection measures. To reduce costs, SCADA systems have replaced many line maintenance personnel familiar with controlled system operation and able to keep the systems running manually in the event of major failures. Many utilities have not yet realized that their systems are accessible via the Internet. SCADA administrators often believe that since their SCADA systems are not connected to corporate LANs they are immune to outside attacks. But since RTUs often transmit and receive through lowest cost third party data links such as the public switched network, leased microwave links, or satellite relays, they are still susceptible to intruders.

The recent National Academies report on the role of science and technology in countering terrorism[2], identified SCADA protection as one of the most important near term technical initiatives that can be accomplished by applying existing technologies. As a first step, computer security guidelines should be strictly enforced for SCADA computer networks. Legal incentives need to be developed to encourage utilities to implement protection measures. Companies need to encourage communication and teamwork among IT security and industrial automation personnel. Risk assessments and red team evaluation of critical infrastructure control systems by technical experts will be important to identify problems and countermeasures. Industry should improve physical security and protection of critical SCADA and RTU locations. Effective government assistance and incentives will be important to encourage implementation of security improvements. Universities can assist by developing education and training programs on SCADA system operation, susceptibilities, and protection measures.

The CIP Project is developing legal and technical solutions that will improve our ability to assess and protect critical SCADA systems. JMU is developing a risk assessment model that focuses on network security for critical infrastructure systems. GMU is investigating legal and policy measures to energize infrastructure owners and operators to protect their critical networks. Results of both efforts will be applicable to ensuring reliable SCADA system operation. ◆

[1] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," Washington Post, June 27 2002

[2] Committee on Science and Technology for Countering Terrorism, <u>Making the Nation Safer</u>, National Research Council, National Academies Press, 2002 <www.nap.edu>

Dr. George Baker is the Interim Director of the Institute for Infrastructure and Information Assurance.

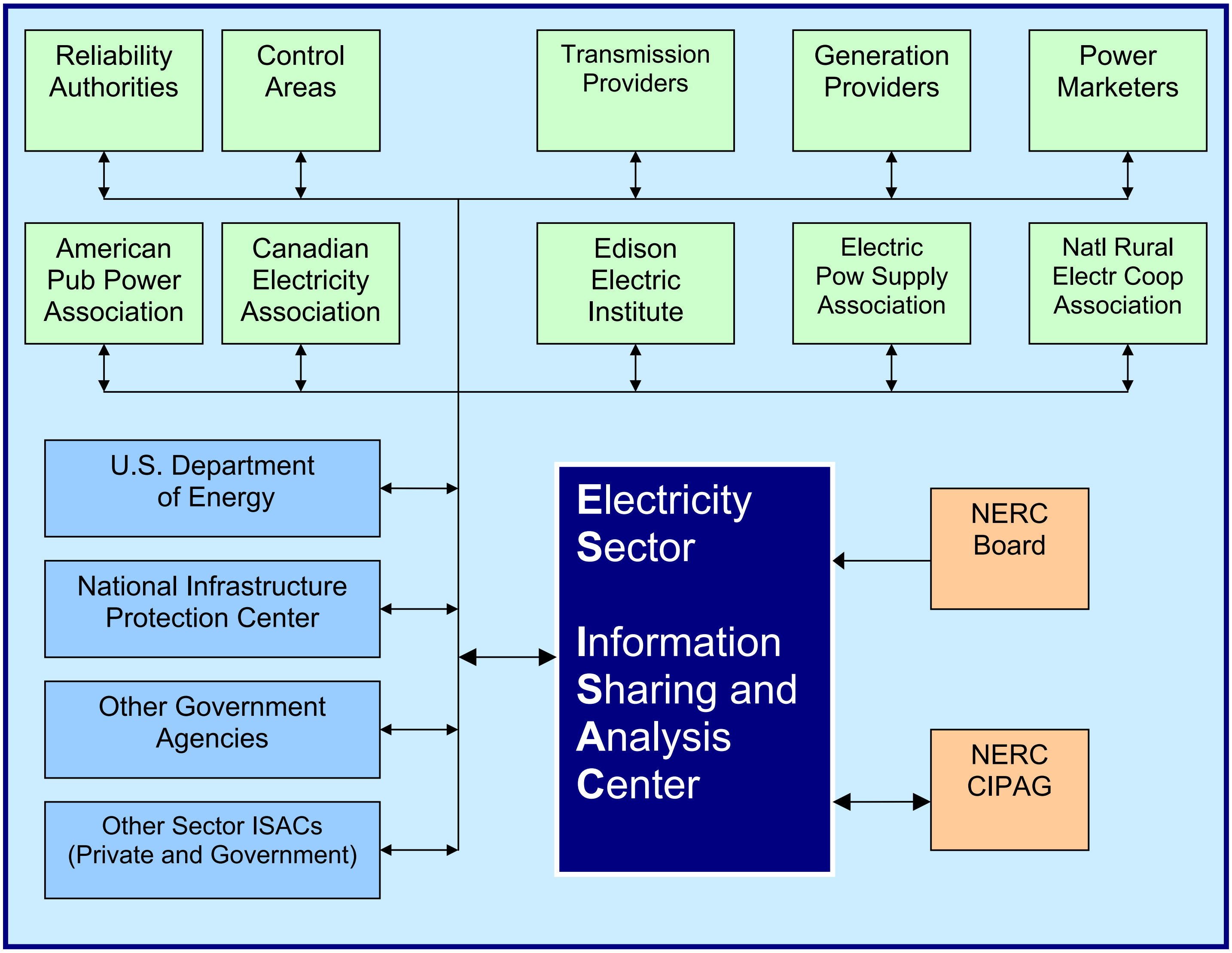
Allan Berg is the Associate Director of the Institute for Infrastructure and Information Assurance.

Electricity Sector Information Sharing and Analysis Center (ES-ISAC)

The North American Electric Reliability Council announced the ES-ISAC in October 2000. The ES-ISAC was formed to:

- Obtain security information related to possible threats or suspicious activity, or actual malicious or terrorist acts against the Electricity Sector and to assure that this information is provided to the NIPC for analysis.
- Assist the NIPC in its analysis of the actual or potential impact of threat to or vulnerabilities of the Electricity Sector. Subject matter expertise may be provided directly by ISAC personnel or through contact with Sector people arranged via the ISAC.
- Immediately disseminate threat and vulnerability warnings on a Sector, geographic, facility type, specific facility basis as appropriate.
- Provide ongoing Sector awareness to the ever-changing security landscape.

The ES-ISAC is staffed by NERC personnel who consult with particular subject matter experts throughout the Sector. The CIP Advisory Group provides functional oversight to the ES-ISAC, which is funded as part of the NERC budget. There are no fees for participating Electricity Sector entities. ◆


Reliability Authorities
Control Areas
Transmission Providers
Generation Providers
Power Marketers
American Pub Power Association
Canadian Electricity Association
Edison Electric Institute
Electric Pow Supply Association
Natl Rural Electr Coop Association
U.S. Department of Energy
National Infrastructure Protection Center
Other Government Agencies
Other Sector ISACs (Private and Government)
Electricity Sector Information Sharing and Analysis Center
NERC Board
NERC CIPAG

***FERC**, continued from page 2*

industry in the North American Electric Reliability Council, Critical Infrastructure Protection Advisory Group (NERC CIPAG). In collaborating closely with the NERC, the FERC has focused on creating cyber security standards as a "generic and least common denominator" – not industry best practices. The FERC has focused on the importance of creating a minimum level of protection for participants in wholesale transmissions.

- **Dam Safety and Security**

The FERC has quietly engaged owners and operators of the nation's dams in developing more enhanced security and safety programs. In addition to working directly with industry owners, the FERC has also partnered across government with other experts – such as the Army Corps of Engineers and the Department of the Interior. The FERC has formed a hydro security team focusing on hydroelectric power projects. The FERC offers guidance to licensees on -

- Risk assessment materials and initial assessments
- Integration of security enhancements with emergency action plans
- Rapid alert notification and dissemination methods
- Training ◆

The Federal Energy Regulatory Commission: Other Useful Links

FERC Website
http://www.ferc.gov/

Electric Power Regulation
http://www.ferc.gov/Electric/electric.htm

Enabling Legislation and Regulation:
http://www.ferc.gov/informational/enable1.htm

Links to Electric Energy Sites:
http://www.ferc.gov/Electric/electricsites.htm

Testimony on Energy Infrastructure by the Chair, Pat Wood, III:
http://www.ferc.gov/news/congressionaltestimony/WoodTestimony07-24-02.pdf

Pat Wood, III
Chairman
FERC

Mr. Wood was nominated to the Commission by President George W. Bush and confirmed by the Senate in 2001. His term expires June 30, 2005. Before joining the Commission, Mr. Wood was Chairman of the Public Utility Commission of Texas. He has worked as an engineer with Arco Indonesia and as an attorney with the Baker & Botts law firm in Washington, DC. He also served as legal counsel to the Chairman of the Texas Railroad Commission. In the early 1990s, he was legal advisor to FERC Commissioner Jerry J. Langdon. Throughout his career, he has worked to advance a pro-customer, market-oriented vision of utility regulation

Pacific NorthWest
Economic Region

BLUE CASCADES
Infrastructure Interdependencies Exercise
Dr. Paula Scalingi

More than 150 representatives from 70 private and public sector organizations attended the first of its kind multi-jurisdiction, cross-border tabletop infrastructure interdependencies exercise. The exercise was conducted by the Pacific NorthWest Economic Region (PNWER) and co-sponsored by the U.S. Navy, Federal Emergency Management Agency (FEMA Region 10), and the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP).

BLUE CASCADES was the second in a series of activities that are elements of a unique initiative — the Partnership for Regional Infrastructure Security — launched by PNWER in late 2001 with the goal of developing a cooperative preparedness strategy using a risk-based approach to enhance the security of critical systems region-wide.

PNWER, chartered in 1991, brings together public and private sector interests with the aim of enhancing the economic development of its eight U.S. and Canadian member jurisdictions: Alaska, Alberta, British Columbia, Idaho, Oregon, Montana, Washington, and the Yukon Territory. The first activity was the Partnership kick-off meeting on Nov. 30, 2001 in Spokane, Washington, attended by over 120 private and public sector organizations from all the jurisdictions that comprise PNWER.

The exercise focused on the linkages between and among infrastructures that could make the Pacific Northwest vulnerable to cascading impacts in the event of an attack or disruption, and which could complicate expeditious response and recovery. Critical infrastructures participating in the exercise included energy (electric power, oil, and natural gas), telecommunications, transportation, water supply systems, banking and finance, emergency services, and government services. Federal, state/provincial, and local government agencies, including emergency management organizations, were also well-represented.

BLUE CASCADES was expressly designed to help stakeholders assess the current state of their understanding and preparedness, particularly from the perspective of infrastructure interdependencies. It also was aimed at identifying their needs, priorities, and resource requirements for incorporation into an Action Plan to assist the eight jurisdictions within PNWER to become a disaster-resistant/resilient region.

During the exercise, players addressed a challenging scenario that was developed by a group of stakeholders representing private and public sectors from PNWER's jurisdictions. Organizations contributing to the scenario included Bonneville Power Administration, BC Gas, BC Hydro, Boeing, Duke Energy, PG&E, Williams Gas Pipeline, Puget Sound Energy, Port of Seattle, Idaho Bureau of Disaster Services, U.S. Navy, the National Infrastructure Protection Center, Telus, Verizon, Qwest, FEMA, BC Provincial Emergency Program, and OCIPEP.

The scenario reflected those threats that the exercise participants were most concerned about — both deliberate and "non-deliberate," with particular emphasis on the type of high-profile terrorist threat that is dominating today's headlines and which could cause cascading, long-term impacts. The terrorist attacks, physical in nature and directed at disrupting the region's electric power, caused region-wide power outages that quickly spread to other western states. There were follow-on disruptions of the region's telecommunications and natural gas distribution, as well as a threat to a major municipal water system and to the region's ports. The attacks and disruptions of

continued on page 15►

Cyber Security Standards in the Electricity Sector

Lee M. Zeichner, Esq.

As part of a landmark Notice of Proposed Rulemaking issued this summer (*see box below*), the FERC has published proposed cyber security "standards" for public utilities servicing "wholesale electric grid operations." The proposed cyber security rules, prepared in large part by the NERC, are set to go into effect in January 2004, but have not been finalized.

This is the first-ever security regulation relating to reliability and assurance of a critical infrastructure service. The cyber-security proposal covers the following elements:

- Application: The new regulations will apply to public utilities as well as certain other service providers; currently both industry and government are examining just how broadly the rules should apply.
- Governance: The rules include a risk and security governance component – focused on accountability in senior management.
- Asset Classification: Security programs must include a process to identify critical assets and functions and to prioritize protection and assurance of those assets.
- Personnel and Access Controls: Social engineering and personnel security are part of the definition of "Cyber Security" in the proposed rules.
- Systems Management: Comprehensive systems security includes software, hardware, and testing. The standards include a range of information and system security guidelines that are acceptable, such as NIST

continued on page 18►

Standard Market Design

On July 31, 2002 the Federal Energy Regulatory Commission (FERC) announced wide-ranging proposals to remedy undue discrimination in the use of the interstate transmission system and give the nation the benefits of a truly competitive bulk power system. In a landmark Notice of Proposed Rulemaking (NOPR) the FERC issued a blueprint for change designed to create genuine wholesale competition, efficient transmission systems, the right pricing signals for investment in transmission, generation facilities and demand reduction, and more customer options. Market monitoring and market power mitigation proposals are also critical parts of the proposals for standardized power market rules.

Standard market design (SMD) is part of a series of initiatives by the FERC to harness the benefits of competitive markets. SMD provides a framework wholesale electric markets to remedy remaining undue discrimination in transmission services and establish a more level playing field between competing generators, loads, and technologies. Under SMD, a majority of the nation's power will continue to be purchased under long-term bilateral contracts, while the rest will be exchanged in organized spot markets for energy and ancillary services. SMD lays out the rules for how those markets will operate, with day-ahead and real-time markets for energy and ancillary services that are linked to the feasibility of actual grid operational capabilities and security.

SMD also defines a new, flexible transmission service, establishes a congestion management system to assure that the grid is managed effectively and that users recognize the true value of their energy use, lays out new rules to assure that all transmission owners and operators recover their costs, establishes new market mitigation and monitoring requirements, and sets out long-term planning and resource adequacy requirements to assure that infrastructure needs are recognized and met without wasteful, dangerous "boom and bust" cycles.

DOE's Energy Security and Assurance Program

From Testimony by Mr. James McDonnell

Director, Energy Security and Assurance Program

The Secretary of Energy has the responsibility as the lead federal agency to coordinate protection activities in the Energy Sector. Presidential Decision Directive 63 assigned this responsibility to DOE and the Secretary expects the Homeland Security National Strategy to continue that assignment of responsibility. The Office of Energy Assurance was established at the Department to better protect against severe energy disruptions in close collaboration with State and local governments and the private sector and, where possible, to assist with emergency response efforts.

The Office provides technical expertise and management oversight to identify energy system critical components and interdependencies, identify threats to the system, recommend actions to correct or mitigate vulnerabilities, plan for response and recovery to system disruption, and provide technical response support during energy emergencies. As originally conceived, the Office has four principle areas of management, which are:

1. Energy Reliability

The Office of Energy Assurance coordinates Department of Energy policy development and intergovernmental, interagency activities related to the protection and reliability of the national energy infrastructure. The Office will utilize longstanding relationships with government and industry representatives to develop a national strategy for energy assurance and establish a national tracking and reporting process to assess the ongoing effectiveness of the national strategy, identifies shortfalls and develops corrective action plans; and coordinates efforts to expand cooperation on national energy infrastructure with friendly nations, international organizations and multinational corporations.

2. Energy Emergencies

The Office of Energy Assurance ensures we are prepared to support states and industry efforts to plan for, respond to and mitigate actions that disrupt the nation’s energy supplies. This Office’s primary missions are twofold; first is the identification of potential threats to the national energy infrastructure, including natural disasters and industrial accidents, and deliberate acts of terror, sabotage. The Office maintains an effective communications and liaison network with the energy sector to facilitate information flow during emergencies and communicate potential and actual threats to the appropriate authorities.

The second mission is to assist in the development of federal energy emergency response plans. In carrying out this function, OEA will provide technical and professional assistance to states and industries for the development of local and regional response plans and conduct readiness exercises with states and industry to assist in identifying shortfalls prior to actual emergencies. Following such exercises, the Office will compile lessons learned during the conduct of emergencies and exercises for broad dissemination among relevant industries and facilities.

3. Energy Infrastructure

The Energy Assurance Team works with the companies whose resources comprise the nation’s energy sector to improve the protection of critical energy facilities. The Infrastructure Office works with the energy sector to introduce new security practices into the energy sector. The Office also interfaces with the DOE laboratory community to help identify and speed commercialization of new technologies designed to enhance the protection of sensitive facilities.

4. Infrastructure Interdependencies

The Office of Energy Assurance

continued on page 13►

Governor Tom Ridge on Working with the Private Sector for Homeland Security

MR. SESNO: Governor, I'm doing some work with George Mason University's critical infrastructure project, and 85 percent of the critical infrastructure of which you speak is owned by the private sector. How is this new department going to work in different ways, once you pull it together, with the private sector, whether it's a chemical plant someplace or an Internet service provider?

GOVERNOR RIDGE: We are close to completing a strategy to deal with -- well, strategy doesn't mean much to folks, so let me just distill it. We've got a way forward so that we can work with the private sector to assess how they're vulnerable, to share best practices, to reduce their vulnerability. And it will be one of the primary functions of this new department because we're going to get a lot of information in, a lot of threat information. We're going to have analysts working -- not only in Washington -- but elsewhere, whose responsibility will be to work with the private sector to shore up those vulnerabilities.

The notion behind the President's initiative -- the notion behind the President's initiative was, first of all we got to map the vulnerabilities in this country. And one of the provisions in the new -- the legislation that created the department was a freedom of information exemption. So that when we're working with the private sector and we're asking them -- and they work very closely with us -- but we need to know where you view yourselves as most vulnerable. That's not exactly information we want to share with the rest of the world. So we have that Freedom of Information Act exemption.

Governor Tom Ridge

We need to do a national overview of our infrastructure, map vulnerabilities, then set priorities, and then work with the private sector to reduce the vulnerabilities based on our priorities. One of the challenges that I think we have -- if you don't mind, Frank, let me just digress here, just a for a minute -- all of us, and we have to fulfill our mission together, all of us -- there is no conceivable way that this country can harden every target, do everything humanly and technologically possible with regard to every person that comes across the border, every piece of cargo that comes across the border, every potential vulnerability in the private sector or the public sector. We can't possibly do that. We're too open. We're too diverse. We're too large. It cannot be done. So the approach that we have to take -- all of us -- is manage the risk. Manage the risk based on vulnerabilities and consequence, manage the risk based on threat information that we receive -- either generated within this country or other sources that we have around the world. There will be a lot of very difficult and challenging decisions that we're going to have to make in this new department. But we have to manage the risk. And we'll do that using your judgment, using the best scientific analysis that we can get. We'll use it doing modeling.

One of the pieces of the new department provides for us to be able to set up some modeling at national labs or academic labs so we can make different assessments about different kinds of vulnerabilities and different kinds of consequences if one of those vulnerabilities is hit. So, again, we're going to manage the risk. We can do it. But I think we just have to remind ourselves that we are a large, open, diverse, trusting country, and we shouldn't kid ourselves as to our capacity of being able to be immune forever from everything. I think we all understand that.

One thing we do know about how the terrorists act, though, you start moving to protect a particular sector or building or target, they'll

continued on page 18►

CYBER DEFENDERS – An Exercise to Educate Tomorrow's Corporate Leaders

by Gerald Martin, Chief, Technical Analysis Branch, JTF-CNO

A crippling cyber attack on the nation's energy infrastructure, a devastating cyber intrusion in the Financial Services Sector….could it have been prevented, how could the sectors have detected it? Those are the issues at the very core of the cybersecurity conundrum.

Scarcely over two years ago, the United States service academies recognized this ominous threat in the cyber arena and designed a Cyber Defense Exercise to enhance the Information Assurance curriculum. With National Security Agency sponsorship, the exercise challenged cadets by teaching information assurance concepts and by preparing undergraduates to "defend the network" against professional security evaluators, known as Red Teams. The exercise required them to not only learn and put into practice the defense in depth concept but also to study and analyze hackers' tools and procedures. Given a variety of platforms and operating systems, the cadets investigated and implemented defensive measures to protect their assets. After a preparatory period, the Red Team attacked their implementations using a pre-determined scoring system and declared the US Military Academy victorious both years.

The Department of Defense (DoD) is not the only network at risk. The private sector and, in fact, DoD, depends enormously on the Internet backbone. It may be prudent for America's colleges and universities to address the critical shortage of information security specialists, indicated by numerous studies and surveys, and what better way than to replicate the enormously successful Cyber Defense Exercise model. ◆

From the Federal Register:

DEPARTMENT OF THE TREASURY:

Study of the Impact of Threat of Terrorism on Availability of Group Life Insurance

SUMMARY: Recently enacted terrorism insurance legislation requires the Secretary of the Treasury (Treasury) to study, on an expedited basis, whether adequate and affordable catastrophe reinsurance for acts of terrorism is available to life insurers in the United States that issue group life insurance, and the extent to which the threat of terrorism is reducing the availability of group life insurance for consumers in the United States. To assist in this study, the Treasury is soliciting comments on a number of questions listed on page 76209 of the December 11, 2002 issue of the Federal Register. Comments must be in writing and received by January 10, 2003.

***DOE**, continued from page 11*

has been designated to provide federal oversight to the National Infrastructure Simulation and Analysis Center as a collaborative effort between the National Laboratories, the Office of Energy Assurance, and other federal agencies. The NISAC, once fully operational, will provide a fundamentally new technical planning and decision support environment for the analysis of critical infrastructures, their interdependencies, vulnerabilities, and complexities for policy analysis and emergency planning. NISAC will use distributed information systems architectures to provide virtual analysis capabilities that will accommodate a large number of providers and a large number of users. Tasking for the NISAC will be developed through an interagency planning process chaired by the Department's NISAC Administrator, which includes representatives of the laboratories and industry and will ensure the NISAC is truly a national asset meet national strategy.

The Department of Homeland Security

The President's legislative proposal creating the Department of Homeland Security includes moving the management of the National Infrastructure Simulation and Analysis Center (NISAC) and other functions of the Office of Energy Assurance from DOE to DHS.

continued on page 14►

Governor Warner Announces Anti-Terrorism and Security Legislation at the CIPP

The Critical Infrastructure Protection Project hosted a press conference given by Virginia Governor Mark Warner on December 9th. Governor Warner announced his anti-terrorism and security legislation, which he plans to propose to the 2003 General Assembly. Congressman Jim Moran and Congressman Tom Davis were also in attendance. The legislation is part of the Governor's overall reform agenda for 2003 and it includes specific security recommendations from his Secure Virginia Panel. "The security of our citizens, our economic well-being and the stability of society depend on our ability to adjust to 21st-century threats," Governor Warner said. "Few responsibilities of government are more important than ensuring public safety and we are moving forward on a number of fronts to put common sense reforms in place."

The legislation includes broad recommendations to enhance Virginia's security in a number of ways. Governor Warner proposed enhanced information sharing between the private sector and the government to ensure continued operation of critical infrastructure in the event of an emergency. Data related to the protection of private and public critical infrastructures would thus be exempted from public release. Second, he proposed improving medical response in the event of an emergency through the development and maintenance of a database of VA medical professionals, liability protections for healthcare providers in the event of a terrorist incident, and drug distribution to citizens on a large-scale. In addition, Governor Warner's plan includes improvements for school safety and enhanced background checks for employees in sensitive positions. Finally, a plan for the leadership of Virginia in a crisis situation is included. This would expand the line of succession in the event that the top leaders were unable to govern.

The Critical Infrastructure Project at George Mason was an appropriate site for Governor Warner to announce his proposed legislation. The Governor's initiatives to enhance security in Virginia are closely aligned with the Project's mission of addressing critical infrastructure issues. ◆

DOE, continued from page 13

The NISAC capability, once established, will provide a unique tool for planning and decision-making. The complexities of the physical and cyber interdependencies associated with the national energy infrastructure are vast by themselves. Once those complexities are overlaid with the other infrastructures, such as telecommunications, the interdependency complexities rise to a level that they become an issue that must be addressed at a national level. The transfer of the NISAC into the Department of Homeland Security will ensure that requirements development and programmatic tasking for NISAC meet national priorities. DOE is planning to transfer funding and two staff members to DHS to provide program oversight for NISAC. DOE will continue to be a customer of NISAC, seeking to utilize this national capability to support Energy Sector analysis.

The transfer of the NISAC administrative functions with the Office of Energy Assurance into DHS will provide the new Department with an integrated management structure to conduct activities associated with protecting the National Energy Infrastructure. The Office also manages a robust vulnerability assessment program that utilizes expertise from the private sector and the National Laboratory complex, plans for and supports restoration and recovery efforts following natural disaster or acts of terrorism, assists states and industry in all aspects of energy emergency planning and supports

continued on page 18►

***Blue Cascades**, continued from page 9*

critical services and related response and recovery actions impacted other interdependent infrastructures, including transportation, emergency services—hospitals, mass care—and law enforcement. Cross-border issues and challenges were highlighted. Relevant operational information provided by a Scenario Design Group made the scenario as realistic as possible.

The scenario provided an impetus for participants to discuss infrastructure interdependencies and infrastructure protection, mitigation, response, and recovery requirements across government agencies and the private sector. Participants grappled with a series of questions that enabled them to explore how a complete disruption or a service curtailment in one infrastructure could cause cascading effects on other infrastructures, and how infrastructure interdependencies could exacerbate repair and restoration efforts.

Overall, participants found that BLUE CASCADES had met its objectives and were grateful for PNWER's leadership and facilitation role in identifying the challenges raised by infrastructure interdependencies. They found the exercise was particularly effective in illuminating what they know and don't know about regional interdependencies, and the preparedness gaps they need to address to create a disaster resistant/resilient region. Participants expressed the need for further such multi-jurisdiction, cross-national activities.

Key Findings

Infrastructure Interdependencies

- Organizations represented demonstrated at best a surface-level understanding of interdependencies and little knowledge of the critical assets of other infrastructures, vulnerabilities, and operational dynamics of these regional interconnections, particularly during longer-term disruptions.
- Many participants initially assumed their organization's contingency plans for addressing natural disasters or isolated emergencies would be adequate in responding to significant terrorist attacks and disruptions and multiple events. However, they came to realize that interdependencies could void or negate those assumptions.
- There was little recognition of the overwhelming dependency upon IT-related resources to continue business operations and execute recovery plans, and the need for contingency plans in the event of loss or damage to electronic systems.

Cooperation and Coordination

- There was minimal coordination of activities and little or no understanding of other organizations' interests, response plans, or restoration priorities.
- There was no region-wide strategy to strengthen security, enhance preparedness, or coordinate emergency response within and across sector and jurisdictional boundaries.
- Law enforcement and industry/private sector cooperation and coordination were limited, with no forum to bring together key law enforcement and security personnel to share information and discuss matters of mutual concern.
- U.S. and Canadian cooperation was seen as limited in the areas of law enforcement, response and recovery and information sharing; at the same time, there was a lack of understanding of what cooperation does exist.
- The range of services that federal civilian and defense agencies could provide during regional emergencies was not clear. Also, information was lacking on how regional national defense facilities, with significant dependencies on commercial infrastructures, would coordinate with these infrastructures.

Communications

- Participants had difficulty envisioning a situation in which they would lose telephonic and internet communication and lacked contingency plans to work around the problem.
- Although many organizations had radio back-up, it was unclear how often these systems were tested. Based on exercise discussions, there would be little if any interoperability with other stakeholder communications systems.
- Law enforcement lacked an effective way to disseminate and receive threat-related

continued on page 16▶

***Blue Cascades**, continued from page 15*

information from private sector organizations and utilities.
- There are no established protocols or regional networks to facilitate rapid and reliable dissemination of outage-related information to critical community organizations and infrastructures.

Resources

- All sectors faced resource constraints to various degrees, including critical components and equipment, and skilled personnel for recovery activities.
- Participants did not take into account the demand on the part of other organizations and businesses to secure scarce additional back-up power generation, including fuel for generators. They also did not appreciate the need to prioritize those demands.

Reporting and Analysis

- There is no common, continent-wide alert system with threat levels that have a corresponding set of actions required.
- The new color-coded alert system established by the U.S. Office of Homeland Security appeared to be little understood, and conflicted with infrastructure sector threat levels.
- There is no mechanism for cross-border sharing of U.S. and Canadian threat- level information or a common color-coded terrorist alert system.
- There are few, if any, regional or industry-sector clearinghouses for threat or incident-related information that can be used for planning and response.
- There are no dedicated communication channels for infrastructure stakeholders to use to report information to federal, state/provincial, and local government agencies to prevent being swamped by requests for status reports.
- Modeling and simulation capabilities do not yet exist that can help assess economic and other damage from prolonged regional disruptions.

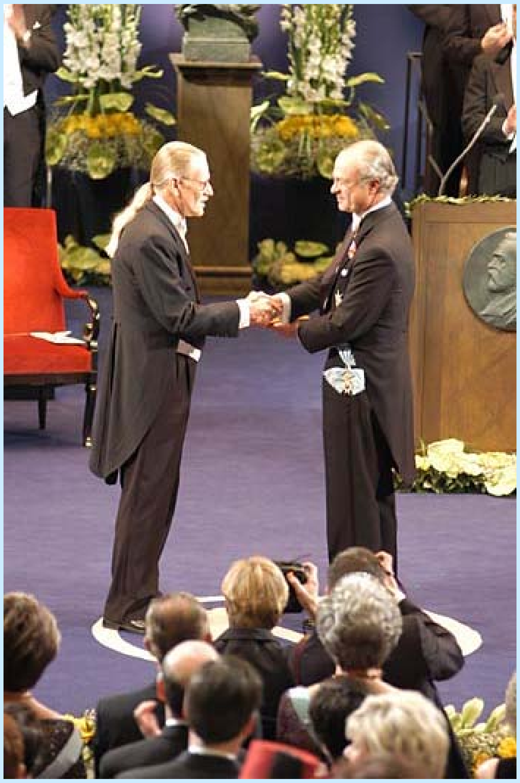
Command and Control

- Roles and missions of the various government authorities at all levels in a large-scale regional terrorist attack or disruption were unclear.
- Participants expressed concern over whether law enforcement should take precedence over restoration, citing designation of critical assets as crime scenes and failure to take into account economic impacts of counterterrorism actions.
- There is a general lack of guidelines on preservation of evidence within private sector organizations.
- Lines of authority were unclear among the FBI and other U.S. and Canadian federal, state/provincial, and local law enforcement entities, including the role of national defense. This was seen as particularly problematical regarding port security.

Public Information

- Coordination and dissemination of public information emerged as one of the greatest challenges

continued on page 17▶



Distinguished CIP Project Scholar Vernon L. Smith receiving his Nobel Prize in Economics from His Majesty the King at the Stockholm Concert Hall. George Mason University is the only school in the Commonwealth of Virginia with two Nobel Prize winners. James M. Buchanan, Jr., Distinguished Professor Emeritus of Economics, was the 1986 Nobel Laureate in Economics.

***Blue Cascades**, continued from page 16*

in a regional infrastructure disaster that involved terrorism.

- Little attention was paid to the all-important "human factor"—that people will panic and believe rumors in the absence of accurate, instructive information.

Selected Recommendations

- ***Improve Understanding of Regional Interdependencies*** by undertaking region-wide identification of what assets are most critical, conducting physical and cyber vulnerability assessments, and identifying/assessing interdependencies.
- ***Develop a regional threat assessment approach*** that takes into account international and domestic adversaries, critical regional assets, and vulnerabilities; leverage work done for Y2K by jurisdictions and the private sector.
- ***State/provincial and local governments should review,*** with private sector input, ***emergency response plans and mutual aid agreements*** to assure that terrorism and interdependencies-related challenges are addressed.
- ***Develop training modules; hold targeted workshops and exercises*** to further address interdependencies issues raised in BLUE CASCADES (e.g., port security; protection of the industrial base).
- ***Develop a secure, regional clearinghouse for interdependencies issues and related preparedness information***, including data on all regional exercises and training opportunities.
- ***Undertake the development of analytic tools to provide credible damage assessments*** for use in preparedness planning and to assist in response and recovery.
- ***Develop a regional nuclear/radiological preparedness program*** that takes into account private and public sector security and response/remediation needs.
- ***Utilize the Partnership for Regional Infrastructure Security to develop a common terminology and preparedness plan for the region***, facilitate exchange of information and monitor the progress of implementation.
- ***Consider the need for a Utilities Regional Security Association (URSA) under the auspices of the Pacific Northwest Economic Region*** modeled along the lines of the California Utilities Emergency Association. URSA would provide a list of regional points-of-contact in all state/provincial, local, law enforcement organizations and utilities, as well as a forum for planning and coordination.
- ***Establish a Maritime Security Coalition as part of a Port Security initiative*** to bring key stakeholders together and address unique port security needs
- ***Foster development of joint U.S.-Canadian protocols, MOUs and collaborative activities*** to address significant law enforcement and consequence management issues, including research and development of analytic tools and technologies to assess regional impacts and mitigate vulnerabilities.
- ***Identify the range of federal civilian and defense resources*** that can be brought to bear to address regional response and recovery needs.
- ***Seek legislative support for necessary policies and technical assistance programs*** to meet regional protection, mitigation, response and recovery needs, including training, exercises; also, information sharing (e.g., relief from freedom of information act and sunshine law requirements).
- Explore options for, and establish, a secure, region-wide common communications network with sufficient redundancy and alternative systems.
- Develop procedures to facilitate the dissemination of outage-related information expeditiously to key infrastructures.
- Establish stockpiles and procedures for prioritized access to electric power generators, other emergency back-up equipment, and also critical components that would be difficult to obtain in the short-term.
- Work with appropriate government organizations to put in place a common, public-private sector, continent- wide, alert system with threat levels that have standardized actions

continued on page 18►

***Standards**, continued from page 10*

guidance and ISO 17,799.

- <u>Security Planning</u>: A program to enhance cyber security planning must now be part of the business process.
- <u>Incident Response & Business Continuity</u>: Seamless restoration of service – always part of the business environment – is now a core requirement in the evolving security framework.

The FERC and the NERC have structured rules to be enforced through a "self-certification" process. According to the proposed rules, companies must begin to self-certify by February 1, 2004. Absent the certification, customers will not be able to receive transmission services, so non-compliance is linked directly to business drivers. The FERC is working with relevant energy sector stakeholders to develop a plan for enforcement of the certification process. NERC has proposed that budgetary constraints will not permit "more than substantial compliance" by FY 2004 and has proposed a FY 2005 deadline for robust compliance expectations. ◆

***Ridge**, continued from page 12*

pull back. And we're going to have to start thinking internally like terrorists from time to time. But around this whole enterprise is the notion of all of us working together to manage the risk. ◆

(From Remarks at a Town Hall Meeting for Future Employees of the Department of Homeland Security held December 17, 2002 in Washington, DC)

***Blue Cascades**, continued from page 17*

required.

- Set up a region-wide, cross-border threat information exchange mechanism and threat data repository.
- Delineate roles and missions of government authorities in regional terrorist-initiated disruptions.
- ***Develop guidelines for law enforcement and private sector organizations*** outlining crisis and consequence management procedures and priorities.
- ***Develop guidelines for effective and expeditious dissemination to the public of information about outages***, including duration, resulting safety factors, and providing instructions on what they should and should not do. Development of such procedures should take the "human factor" into account.
- **Establish a mechanism to coordinate public information during regional emergencies.** ◆

Frank Sesno
CIP Project Fellow

***DOE**, continued from page 14*

the development of strategic energy policies. The new Department of Homeland Security will thus have the ability to directly access the expertise associated with the Office of Energy Assurance and the national laboratories for assessments of the energy sector. In addition, the new Homeland Security Centers for Excellence will provide the Department with direct access to the capabilities currently resident in the national laboratories for research and analysis in other areas of the nation's critical infrastructure. ◆

The CIP Report is published by LegalNet Works, Inc. on behalf of the CIP Project. Formed in 1996, LegalNet Works Incorporated focuses on the development of information security laws and regulations with an emphasis on liability, risk management, national security, regulatory compliance, and privacy. LegalNet consults both government and industry officials on legal and policy reform in these complex areas.

If you would like to be added to the distribution list for *The CIP Report,* please send an e-mail to cipp01@gmu.edu.