JANUARY 2004 / VOLUME 2, NUMBER 7

THE CIP REPORT

Developments in the CIP Arena

CIP Project Staff

John McCarthy, *Executive Director*

Emily Frye, *Associate Director, Law and Economics Programs*

Kevin "Kip" Thomas, *Associate Director, Research Programs / Research Associate Professor*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click here.

The field of critical infrastructure protection is constantly evolving with new research, partnerships, and policies, but it seems that the last 60 days have been particularly noteworthy for the number of developments taking place. In December the President issued Homeland Security Presidential Directive-7, which replaced the heretofore most influential document in the federal CIP arena, Presidential Decision Directive-63, signed by the Clinton Administration in 1997. HSPD-7 shifts significant responsibility for achieving CIP national policy objectives to the Department of Homeland Security.

DHS' Information Analysis & Infrastructure Protection Directorate has been appropriately busy ratcheting up its CIP operation, specifically with the creation of the National Cyber Security Division and the US-CERT. NCSD is charged with coordinating the implementation of the National Strategy to Secure Cyberspace and serves as the single national point of contact for the public and private sector regarding cyber security issues. NCSD's US-CERT serves as a focal point--bridging public and private sector institutions--to advance computer security preparedness and response. The late-January announcement of the first National Cyber Alert System, a program offering information products in the form of e-mail alerts and tips to home users and security experts alike, is a testament to the agency's commitment to proactive and tangible progress in CIP.

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

Developments in critical infrastructure protection are ongoing even as this issue of *The CIP Report* goes to publication-cyber security experts deal with a major digital attack by the MyDoom virus, and policy experts await the release of the final National Response Plan.

This issue of *The CIP Report* provides information on some of these developments, as well as other significant initiatives in the CIP world. We are also very pleased to provide an excerpt of a "Critical Conversations" segment with Frank Sesno. We hope that you find this issue informative, and we at the CIP Project wish our readers a happy, safe, and successful year in 2004.

New Directive Replaces PDD-63, Restructures CIP Responsibilities

On December 17, 2003 President Bush released the Administration's policy on critical infrastructure protection. In replacing Presidential Decision Directive 63, the Clinton Administration's infrastructure policy, Homeland Security Presidential Directive 7 (HSPD-7) crowns the Department of Homeland Security as the focal point for achieving national policy objectives. In this capacity, DHS is empowered to prioritize and coordinate infrastructure protection activity and to manage the flow of threat information to industry stakeholders. As a decision directive, HSPD-7 requires Federal government agencies to marshal resources and collaborate to achieve articulated policy objectives.

Each Federal agency now has until July 2004 to develop an infrastructure plan that identifies all of an agency's critical infrastructure and includes plans for prioritization, protection, recovery, and reconstitution of systems or resources. The PDD-63 deadline for submitting these plans to the Office of Management and Budget was October 2003. But a Congressional committee headed by Rep. Adam Putnam has found agencies to be far behind in identifying their critical information systems.

The presidential directive merges two distinct policy objectives: (1) Protecting key resources and infrastructures from terrorist attack and (2) Preventing infrastructure disruptions and restoring services where terrorism is not an issue. However, the principal emphasis of the directive is on terrorism and empowering DHS to "identify, prioritize, and coordinate" protection strategies. The directive does not clearly outline responsibility for assuring reliability of service and managing widespread infrastructure disruptions where security issues are irrelevant.

Like PDD-63, the Administration assigns single government agencies to manage public-private infrastructure activities. HSPD-7 departs significantly from PDD-63 in assigning responsibility for the following infrastructure sectors to DHS:

- Information Technology (previously Department of Commerce);
- Telecommunications (previously Defense Department);
- Chemical (previously Environmental Protection Agency);
- All transportation systems previously Department of Transportation); and
- Postal and Shipping (newly created Sector).

The directive uses "Sector-

(Continued, Page 4)

Sector - Specific Agencies

Agency	Sector
Department of Agriculture	agriculture and food (meat, poultry and egg products)
Health and Human Services	healthcare and food (other than meat, poultry and egg products)
Environmental Protection Agency	drinking water and water treatment systems
Department of Energy	all energy assets, excluding commercial nuclear facilities
Department of the Treasury	banking and finance
Department of the Interior	national monuments and icons
Department of Defense	defense industrial base

U.S. CERT to Coordinate National Cyber Incident Response

The Department of Homeland Security recently announced the creation of the U.S. Computer Emergency Readiness Team (U.S. CERT) as a streamlined center for incident response. The U.S. CERT is a partnership between DHS's National Cyber Security Division, formed in June 2003, and Carnegie Mellon's Computer Emergency Response Team (CERT-CC).

The US-CERT, which operates 24/7, will complement current security capabilities, including the Federal Computer Incident Response Center (FedCIRC), which coordinates incident warning and response information across Federal Civilian Government agencies. Partnering with the CERT-CC will expand DHS's capabilities for providing cyber analysis, warning and response coordination including:

Improving Warning and Response to Incidents

By fostering the development of open standards based security event detection methods and tools, in collaboration with the private sector and leading response organizations, the US-CERT will improve warning and response times. The US-CERT and its partners will utilize common commercial incident and vulnerability reporting protocols to increase the flow of critical security information throughout the Internet community. A security extranet will provide near real-time dissemination of warnings and response capabilities.

Increasing Coordination of Response Information

The US-CERT will provide a coordination center that, for the first time, links public and private response capabilities and facilitates communication across all infrastructure sectors. The US-CERT will work with private sector companies to promote the development of enhanced response and warning technologies and services in order to ensure that consumers and businesses have access to such capabilities.

Reducing Vulnerabilities

US-CERT will collaborate with the private sector to develop and distribute new tools and methods for detecting, identifying, and remediating vulnerabilities.

Enhancing Prevention and Protection Efforts

US-CERT will improve incident prevention methods and technologies by identifying and disseminating *(Continued, Page 12)*

National Cyber Alert System

On January 28 the National Cyber Security Division announced the National Cyber Alert System, an operational system delivering to Americans timely and actionable information to better secure their computer systems.

As part of this program, Homeland Security is making available a series of information products targeted for home users and technical experts in businesses and government agencies. These e-mail products will provide timely information on computer security vulnerabilities, potential impact, and action required to mitigate threats, as well as PC security "best practices" and "how to" guidance.

This new National Cyber Alert System is America's first coordinated national cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. Managed by U.S. CERT, the system provides the first infrastructure for relaying graded computer security update and warning information to all users.

The new National Cyber Alert System security suite of products includes:

Cyber Security Tips: Targeted at non-technical home and corporate computer users, the bi-weekly Tips provide information on best computer security practices and "how-to" information.

Cyber Security Bulletins: Targeted at technical audiences, Bulletins provide biweekly summaries of security issues, new vulnerabilities, potential impact, patches and work-arounds, as well as actions required to mitigate risk.

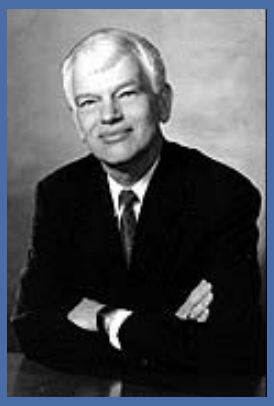
Cyber Security Alerts: Available in two forms - regular for non-technical users and advanced for technical users - Cyber Security Alerts provide real-time information about security issues, vulnerabilities, and exploits currently occurring. Alerts encourage all users to take rapid action.

All information products are available on a free subscription basis and are delivered via push e-mail. Sign up for the alert system at www.us-cert.gov.

Message from Dr. Alan G. Merten President, George Mason University

It is with pleasure that I announce that Congress has appropriated the third $6.5 million round of funding to support the work of the CIP Project. This funding, provided through the National Institute of Standards and Technology at the Department of Commerce, is a testament to the work of faculty and staff at George Mason University, our partner James Madison University, and all the participating universities. Our efforts have contributed significantly to enhancing the security and economic processes supporting our cyber networks and the nation's critical infrastructures.

Last year was an exciting time for the Project - a number of new academic research initiatives were undertaken and proceedings from our first annual "CIP Workshop I Working



Papers" was published. Additionally, several national forums focused on education and outreach including two Critical Conversations ('Protecting America's Critical Infrastructure: From War Room to Boardroom' and "Power Play: Protecting the Electric Grid') led by Frank Sesno with senior government and policy makers focusing on this important national concern.

I am confident that in its third year the CIP Project will continue to advance the dialogue about critical infrastructure protection and homeland security through continued research, educational opportunities, and outreach programs. Many challenges, both old and new, confront policymakers and business leaders in this important arena. The CIP Project has established that academe can make a major contribution to success. ❖

HSPD-7 *(Cont. from Page 2)*
Specific Federal Agencies" to clarify roles and responsibilities for collaborating with private sector owners. Responsibilities include collaborating with key industry stockholders, conducting or facilitating vulnerability assessments of the sector, and encouraging risk management strategies.

HSPD-7 further requires DHS to serve as the focal point for the security of cyberspace. At this time, the National Cyber Security Division, and the US-CERT, provides these coordination mechanisms. The Office of Management and Budget as well as the CIO Council share the responsibility with regard to Federal government infrastructure protection.

Three new coordination challenges for critical infrastructure will garner increasing attention in the next year: (1) Creation of a geospatial policy for critical infrastructure protection; (2) Development of a national indications and warning capability; and (3) Requirement to link critical infrastructure plans to budget requests. ❖

GILMORE COMMISSION ISSUES FIFTH AND FINAL REPORT

Calls for Improved Homeland Security Strategy

According to the Gilmore Commission report released in December, the United States needs an improved homeland security strategy to strengthen security in communities facing the greatest risk, improve the use of intelligence, increase the role of state and local officials, and sharpen disaster response capabilities.

In a report to President Bush and the Congress, the commission-chaired by former Virginia Gov. James S. Gilmore III-says the creation of the Department of Homeland Security has resulted in improved planning and readiness. But the report concludes that the overall national homeland security strategy should be directed by a White House-level entity that "must have some clear authority over the homeland security budgets and programs throughout the federal government."

The Gilmore Commission says that an existing entity-the Homeland Security Council-is best equipped to craft a new strategic policy that could then be carried out by the Department of Homeland Security, other federal agencies and a host of state, local and private groups that also must be involved. The Homeland Security Council is made up of the secretaries and heads of federal departments and agencies with homeland security responsibilities, supported by its own staff in the White House.

The formal title of the federally chartered Gilmore Commission, created in 1999, is the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. The RAND Corporation provides staff support to the commission.

We must resist the urge to seek total security-it is not achievable and drains our attention from those things that can be accomplished.

James S. Gilmore

The 17-member Gilmore Commission will disband in early 2004 now that its final report is complete. Since it began, the panel has made 144 recommendations, with 125 being adopted by the Congress and various government agencies.

The commission says that by providing long-term guidance to federal, state, and local government officials, an improved homeland security strategy can help create a "new normalcy" that acknowledges the threat of terrorism will not disappear, but still preserves and strengthens civil liberties. "There will never be a 100 percent guarantee of security for our people, the economy, and our society," Gilmore writes in the report's cover letter. "We must resist the urge to seek total security-it is not achievable and drains our attention from those things that can be accomplished."

The commission calls on the president to create an independent, bipartisan oversight board to provide counsel on homeland security efforts that may impact civil liberties, even if such impacts are unintended. The commission says the board is needed because of the potential chilling effect of government monitoring conducted in the name of homeland security. The report expresses concern about protecting freedoms guaranteed by the First Amendment to the Constitution, which could be violated by government's increased reliance on sophisticated technology that has vast potential to invade personal privacy.

The Gilmore Commission urges policymakers to move beyond simply reacting to the Sept. 11 terrorist attacks. The report calls for forward-thinking efforts by government at the federal, state and local levels, and by the private sector as well. Despite an encouraging start in the effort to protect the nation against terrorism, the report warns that "the momentum appears to have waned as people, businesses,

(Continued, Page 6)

Gilmore *(Cont. from Page 5)* and governments react to the uncertainties in combating terrorism and to the challenge of creating a unified enterprise."

The Gilmore Commission says that one important element of a national strategy for homeland defense should be to empower state and local officials, who have been drafted into the homeland security efforts in an inconsistent manner. To ease the confusion experienced by local and state governments and others seeking aid from the Department of Homeland Security, the commission calls for creation of a single grant-making entity in the department to streamline a funding process that now involves many units.

Another Gilmore Commission proposal designed to assist localities calls on the Department of Homeland Security to revise its color-coded Homeland Security Advisory System to include a way to notify local and regional emergency responders about threats to their specific jurisdictions. A revised alert system also should include training to show emergency responders preventive actions necessary at different threat levels, the commission says.

A RAND survey of 918 state and local emergency response agencies (such as law enforcement departments, fire departments, emergency medical services, hospitals, emergency management agencies and public health agencies) conducted for the Gilmore Commission found that state-level organizations are relatively positive about federal homeland security efforts up to now. However, the survey found that local response organizations are less satisfied.

While the RAND survey found that state and local emergency response organizations want more federal funds for their homeland security efforts, the Gilmore Commission cautioned against increasing aid without first developing a mechanism that would give priority to the regions where the risk is greatest and without implementing measures to make sure money is being spent wisely.

"The system does not have to be built on the premise that every community in America must have the same type and the same level, based almost exclusively on population considerations, of response capabilities" the report says. "The panel firmly believes that one size does not fit all." Risk assessments that look at a variety of factors-including population-should eventually become the basis for allocating funding, the Gilmore Commission recommends. Those efforts should be backed up by the creation of an improved mutual aid system that allows for a quick and effective response should disaster strike, the commission says.

According to the report, too little intelligence information is shared with state and local officials, despite improvements in the ways the government handles such information. The Gilmore Commission recommends that to improve intelligence sharing, the president should: designate a federal authority that can speed up the granting of security clearances for state, local and private officials; provide training to allow these officials to use intelligence information; and overhaul the current classification system to improve the dissemination of critical intelligence.

Members of the Gilmore Commission represent fire services, emergency medical services, law enforcement, emergency management, public health, the medical community and local government. They include former senior federal officials and senior retired military officers. One of the members was Ray Downey, who died in the collapse of the second World Trade Center tower in the Sept. 11, 2001 terrorist attacks. Downey was deputy chief and chief-in-charge, special operations, for the New York City Fire Department.

The Gilmore Commission report is the product of a series of meetings and workshops that the commission has held over the past year. In addition, the report includes findings from several research projects conducted by analysts at RAND, and detailed results from RAND's nationwide survey of state and local emergency response entities. ❖

LEGAL INSIGHTS

by Emily Frye

When Subjective Values and Objective Rights Collide: Leveraging the Fourth Amendment to Tailor Privacy Rights

by Guest Columnist Joseph Decker
George Mason University School of Law and Winner, The Murphy Prize 2003

Two weeks after the September 11, 2001 attacks, Attorney General John Ashcroft explained the need to change the rules that control how law enforcement agencies collect domestic intelligence. "Technology has dramatically outpaced our statutes. Law enforcement tools created decades ago were crafted for rotary telephones - not email, the internet, mobile communications and voice mail. Every day that passes with outdated statutes and the old rules of engagement is a day that terrorists have a competitive advantage. Until Congress makes these changes, we are fighting an unnecessarily uphill battle."[i] One month later, the President signed the USA PATRIOT Act (the Act)[ii] into law.

The Act provided updates that extended existing law to modern technologies. For example, the Act expands statutes to trace telephone numbers of incoming and outgoing calls on a suspect's phone (pen register, trap and trace or a "PR/TT.") The updated PR/TT statute could track the sender and receiver of emails and lists of URL sites returned by searches under targeted internet and email accounts. In order to obtain a PR/TT, the law enforcement agency must certify "that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[iii] This lower standard evades the warrant requirement typically associated with such interception under the Fourth Amendment and expands the scope of personal data that falls outside the amendment's protection. Already low privacy rights further dwindle under the Act. *Can privacy be protected and still allow law enforcement agencies to gather necessary information?*

One of George Mason School of Law's most popular professors, the late Richard S. Murphy, provided a brilliant study of this problem in a commercial context in his paper *Property Rights in Personal Information: An Economic Defense of Privacy* (1996).[iv] Law and Economics analysis tends to discount the value of privacy, especially as a protection for reputation, because less information almost invariably increases transaction costs. However, Professor Murphy noted that some individuals value their own privacy very highly, beyond concern for reputation. He asserted that this subjective value should be considered when evaluating privacy.

He cited two examples. William Sidis, a former mathematical prodigy had elected to live his life in seclusion and anonymity until a 1937 James Thurber piece in the New Yorker revealed his whereabouts and habits. Sidis sued the New Yorker and lost.[v] Second, in 1984, Oliver Sipple thwarted an assassination attempt on Gerald Ford and the publicity resulted in the San Francisco Chronicle revealing that he was homosexual. Sipple had chosen not to reveal his sexual orientation to his family or some of his friends. He also sued and lost.[vi] Professor Murphy concluded that lawsuits as a legal remedy inevitably failed to protect individuals who valued their privacy highly, because such privacy torts relied on objective standards of privacy. For William Sidis and Oliver Sipple, an objective standard would not cover the information that others had exposed about them.

Professor Murphy proposed that the most economic way to balance the need for information with the desire for privacy would be to replace tort rules with property rights and let individuals negotiate their own privacy as they chose. Professor Murphy illustrated this idea using an example of voluntary transactions *(Continued, Page 8)*

Legal Insights *(Cont. from Page 7)* between consumers and merchants. Merchants subsequently use (and even sell) the information they obtain when a consumer purchases from them. This became a widespread issue with the advent of internet sales because the email address of the consumer automatically went with the transaction. One purchase on the internet begets a flood of similar, often unwanted offers. Professor Murphy argued that a consumer's privacy could be protected by setting a default rule for non-disclosure of information obtained in voluntary transactions. The merchant could then "purchase" the right to use the information by offering lower prices or other incentives. Both merchant and consumer benefit. Consumers who value their privacy highly can keep it. Merchants can create target advertisements limited to customers who want additional offers without offending those who do not. Those who normally might not want further merchandise could opt to give up their "privacy" for the right incentive.

Many of the expansions of the U.S.A. P.A.T.R.I.O.T. Act can be analogized to the transactions Professor Murphy examined. Like merchants, the government acquires information from an individual's voluntary transactions such as sending an email, searching for URL's or making a telephone call. The individual cannot contract ex ante with the government as he could with a merchant, but instead relies on Constitutional limits on the government's access to information: the Fourth Amendment.

Unfortunately, the Fourth Amendment creates a weak and inadequate default rule to assign a property right, especially with the PR/TT statute. First, the amendment creates no warrant requirement for PR/TTs. Second, where it applies, the amendment attempts to protect privacy interests by making illegally obtained evidence inadmissible at trial. Thus the Fourth Amendment provides no remedy for the innocent person who has no evidence to suppress. Alternative remedies for injunctions or Bivens suits generally fail to provide deterrence or compensation.[vii] Finally, the standard used to define a Fourth Amendment search is objective: a "reasonable expectation of privacy." Professor Murphy's conclusions about the privacy tort apply equally to the Fourth Amendment - highly valued subjective rights cannot be adequately protected by objective standards.[viii]

In the wake and reexamination of the PATRIOT Act, Professor Murphy's solution to privacy rights can be applied if Congress assumes a more active role in protecting privacy rights (rather than relying on the Supreme Court to do so). Congress itself defined the lower standard of proof required to grant a PR/TT. Congress could redefine the standards for a PR/TT to default to Fourth Amendment protection and require probable cause before granting an order for one. Congress would then give a tax credit to internet service providers who offer services subject to the (current) lower standard, or even allow this discounted level to operate as a complete waiver for PR/TT's.[ix] The ISPs could sell less protected services at a lower price. A subscriber who opts to maintain the higher-priced "probable cause" internet service would have stated his preference for privacy and any PR/TT request against him would then fall under the Fourth Amendment. Those who opt for the less expensive service have assented to being held to a lower standard.

Creating a higher default standard and providing incentives to relinquish it solves numerous problems that cannot be addressed by the Fourth Amendment. The individual can decide whether his privacy is worth the price difference between more or less protected internet service. The approach provides ex ante compensation (lower ISP costs) to those who might lose their privacy but who would not normally have a chance for redress. Finally, law enforcement agencies would be restrained from applying PR/TT's to protected internet service providers only when they could not establish probable cause for the PR/TT request.

[i] *See* #9-25-01: Attorney General John Ashcroft Testimony before the Senate Committee on the Judiciary , available online at http://www.usdoj.gov/ag/testimony/2001/0925AttorneyGeneralJohnAshcroftTestimonybeforetheSenateCommitteeontheJudiciary.htm (last visited January 19, 2004.)

[ii] Uniting and Strengthening America By Providing Appropriate Tools Required to

(Continued, Page 13)

Looking Ahead to 2004

Dr. John B. Noftsinger, Jr.
Associate Vice President for Research and Public Service
Executive Director, Institute for Infrastructure and Information Assurance
James Madison University

Critical infrastructure protection is a vast area of responsibility, touching all of our core societal components and creating the fabric of our daily lives. For those of us immersed in the ongoing efforts to improve our national security and the stability of our future, 2004 holds new issues and problems that will keep us moving forward. It is important to take note of our accomplishments and lessons learned, while maintaining focus on the challenges that will occupy the year ahead and our future.

We have had the mixed blessing of having our critical infrastructures placed in an unprecedented position of public awareness and scrutiny during the past year, exposing our vulnerabilities and interdependencies, but also educating and creating awareness of the challenges everyone in critical infrastructure protection faces. Many of our critical infrastructures received national media coverage following the Northeastern Blackout and the aftermath of Hurricane Isabel, both of which highlighted our reliance on a vulnerable electric power grid and the many infrastructure interdependencies that exist between sectors. Yet despite the difficulties these events caused, much has been learned about our vulnerabilities, including mitigation, communication and coordination strategies that go beyond any one sector or infrastructure. These lessons will provide the building blocks for the challenges in the future and now highlight our path forward.

Dr. John Noftsinger

The cyber attacks that disrupted our communication and crippled our computing capacity provided a much needed reminder that as we focus our efforts in physically buttressing and strengthening our critical infrastructures, we cannot minimize the importance of cyber security. The Slammer and Sobig attacks were far more than disruptions or inconveniences; they were rude reminders that we must balance physical and cyber security if we are to truly protect our critical infrastructures. In much the same manner, as we focus on the complex systems we have created that support our daily needs, we must also examine the heath care system that struggles in the wake of such outbreaks as Anthrax, SARS, and most recently, the flu. Simulations and table top exercises such as Dark Winter illustrate the potential for a health outbreak which could cripple the health industry, as well as other components of society, triggering mass panic. While our critical infrastructures represent complex systems that require continual attention, we must remember to focus on all sectors, and not just in times of calamity and exploited vulnerability.

For many new to this field, these events raised awareness towards one of the most difficult problems we face. While the government is tasked with keeping our nation safe, private industry owns more than eighty percent of our critical infrastructure. Despite the complexity this adds to the process, much effort has been put into bridging the gap between these groups on the part of the ISACs (Information Sharing and Analysis Centers formed by PDD-63). The work done between the ISACs and DHS has steadily improved the communication and mitigation efforts required to move us forward to a more secure future and deserves recognition. Both together and separately these groups have made enormous progress in coming together, *(Continued, Page 13)*

Power Play: Protecting America's Electrical Grid

On November 19, 2003 the Critical Infrastructure Protection (CIP) Project hosted "Power Play: Protecting America's Electrical Grid", the second in a series of Critical Conversations hosted by the CIP Project. As was made evident in recent events, such as the Northeast blackout and Hurricane Isabel, the state of the national power grid is of extreme national concern

This second in the "Conversations" series brought together six distinguished panelists, including senior policy makers and industry executives. These leaders in their field provided their insight and helped to shed light on a simple question that has no simple answers, "What needs to be done to make the supply of electricity in this country - from generation to transmission - as well as the electric grid, more secure and more reliable?"

The esteemed panel included Anna Aurilio, Legislative Director of the United States Public Research Group (U.S. PIRG); John Derrick, Chairman of PEPCO Holdings, Inc; Michehl Gent, President and CEO of the North American Reliability Council (NERC); Congresswoman Loretta Sanchez (D-CA) of the U.S. House of Representatives; Denise Swink, Acting Director of the Office of Energy Assuredness, U.S. Department of Energy; and, Patrick Wood, Chairman of the Federal Energy Regulatory Commission (FERC).

John McCarthy, Executive Director of the CIP Project, began the event with opening remarks. Subsequently, Frank Sesno, moderator of the event and GMU Professor of Public Policy and Communiation and senior fellow on the Critical Infrastructure Protection Project, directed the conversation to the security and reliability of the nation's power grid and how to improve it. Following are brief excerpts from the discussion.

Mr. Sesno: Please comment on the Northeast Blackout of August 2003. What should be our top priorities?

Patrick Wood, Chairman, Federal Energy Regulatory Commission:

I think it is important to consider just how secure and reliable the electrical grid is today. We are talking about a very robust three-country grid in North America that already has very high reliability. When you think about 50 million people losing power, the truly high reliability is hard to remember.

The report from the Northeast Blackout will lay out with great detail what happened at every tenth-of-a-second cycle on the afternoon of August 14th. The propagation of outage and the recovery are dealt with somewhat in this report, but will be highlighted more in the final report, which will ask for public comment and hearings in both the United States and Canada.

It is recognized that the grid is not a lot of independent islands in the sea. It is part of a whole interconnected ocean of electricity, and the interconnectedness of it requires not only cooperation, but some standardization. The rules that apply to the reliability, which Mr. Gent's organization (NERC) has worked with quite a bit over the last 40 years, are very important in tying that all together.

So the utilities need to do their job well but they also need to recognize that in today's environment, which isn't a whole lot different than it was 50 years ago, they are interconnected. The product moves at the speed of light so utilities need to work with each other pretty fast.

Michehl Gent, President and CEO, North American Electric Reliability Council:

We have a number of communications facilities that the operating people use. Over the years we have learned to use these, and we may have become comfortable. We need to decide whether the rules we have are adequate, and if they are adequate, then we need to figure out who broke the rules and why and fix that. It just could be that *(Continued, Page 11)*

Power Play *(Cont. from Page 10)* some of the very basic things that we thought were sacrosanct, were golden, have to be changed. We've designed the system to handle over-current and now maybe we need to redesign the system to handle lack of voltage, or something like that.

So there will be a lot of PhD theses written off of this blackout, but I think when it's all over, we will have not only the best system in the world, and we'll not only maintain that, but we will have one that is infinitely better than it is now.

Mr. Sesno: Can you please comment on the Energy Bill and what may be needed to mandate certain standards.

Denise Swink, Acting Director, Office of Energy Assuredness: The bill is inadequate in putting a regulatory hand on this industry to assure its reliability. Notwithstanding the regulatory issue, I would want to say something that is associated with it from a homeland security perspective, and one of the questions that was already asked, was what lessons did we learn from the blackout? This relates to the energy legislation and it relates to what happens after the blackout.

One thing that we really learned was that clearly mistakes are the first line of reaction to these types of situations. I think what the states learned is that they have become lax in understanding who should know what about an energy disruption, and how it affects other infrastructures.

Michigan just recently came out with their report a few weeks ago, and they really emphasized that. If we are going to use distributed generation as part of a grid of the future, we have to make sure that the units run. They found out in Ohio and Michigan that people had backup generation units, but did not have any contracts for fuels and did not have anyone that knew how to hook it up. There's a part to it besides the regulatory side--how do we get ourselves better prepared for these incidents, whether at the state level or the national level?

Anna Aurilio, Legislative Director, United States Public Research Group: I want to repeat again

about the reliability standards. We are going to be going from something that is voluntary self-regulation on the part of the industry to mandatory self-regulation. It is better to have mandatory than voluntary, but it is still the industry setting the rules and in charge, so in our minds that is not far enough.

Finally, the Energy Bill repeals one of the longest-standing consumer protection laws on the book, the Public Utility Holding Company Act in 1935. That was supposed to prevent things like Enron, only Enron got an exemption. In its place, it actually weakened things like FERC's merger review authority. So it puts no protections in place for consumers and industry will be even less accountable. So we think this takes us backwards.

Mr. Sesno: Repeal of the 1935 Public Utility holding Company Act (PUHCA)-Is this right or wrong, and how do we make sense of this?

John Derrick, Chairman of PEPCO Holdings, Inc.: I think there are two things I would say about this. In terms of the regulated aspect

of our business, the wires business as we call it, it is highly regulated. No one is going to buy a local utility without the approval of the local regulators, which also means the state legislature in a great measure. Because of this, you are not going to see Wal-Mart or somebody buying up a bunch of regulated distribution utilities. The Chairman has spoken to the role he has relative to the bulk power. I am all for the repeal of PUHCA because I think what it will do is allow capital to come into this industry and do some very constructive things.

For example, my power supplier is bankrupt, as are some others, and the notion of having companies like Exxon-Mobil or Shell become active in energy to start to aggregate those kinds of resources and bring stability is in my opinion very positive.
(Continued, Page 12)

Power Play *(Cont. from Page 11)*
I want to see an opportunity for new capital - an affiliated capital. Energy companies have a chance to get involved in the generation in our industry because I think that would be a positive thing, and they are not going to be able to get involved in the distribution, because that is where we serve customers without the local regulators approving it.

Let me just say that I think this Energy Bill, as it pertains to electric reliability, is a major step forward, and we needed a major step forward. This is a crawl, walk, run thing as far as I am concerned. We know today that we can do things better, and we are not doing them better in part because the rules we are operating by do not have sufficient teeth in them.

This bill sets the stage or allows the process to move forward, albeit more haltingly than some of us would like, but it moves us forward in my judgment toward an end that we all share, which is to keep the lights on.

Mr. Sesno: What are the priorities of what needs to be done in order to make this critical infrastructure safer?

Congresswoman Loretta Sanchez (D-CA):  First and foremost, I think we need an inventory of what we actually have out there. We understand that 85% of the entire critical infrastructure that sits in the United States sits in private hands. And coming from the business world, I also have a problem with that too, because as some of my people say to me, if we share information with the government regarding our computer security, then that is just one more place where this information is sitting. It creates an even higher vulnerability for attacks.

The possibility of attack comes from everywhere. It can be a physical attack, it can be a cyber-security attack. We think most often it will be, when it happens, somebody from the inside. So we are sitting there trying to struggle as a Congress and as an administrative agency that the Department of Homeland Security is, and ask how do we get industry to step up to the plate and protect these critical assets to the point where we need it to be, while at the same time we understand that the important thing for business is the bottom line. ❖

U.S. CERT *(cont. from Page 3)*
best practices. In addition, the US-CERT, working with infrastructure owner/operators and technology experts, will foster the development of improved security technologies and enhanced analytical methodologies.

The US-CERT will establish collaborative partnerships with:

- computer security incident response teams (CSIRTs)
- Information Sharing and Analysis Centers (ISACs)
- managed security service providers (MSSPs)
- Internet service providers (ISPs)
- security product and service providers
- other organizations participating in cyber watch, warning, and response functions
- security practitioners

US-CERT partners will agree to share information with each other based on a mutually understood set of data sharing principles. ❖

Amit Yoran serves as the Director of the National Cyber Security Division of the Information Analysis and Infrastructure Protection office at the Department of Homeland Security. Mr. Yoran was most recently the Vice President for Managed Security Services at Symantec Corporation where he was primarily responsible for managing security infrastructures in 40 different countries. Before working with Symantec, Mr. Yoran was the Founder, President and CEO of Riptech, Inc., a leader in outsourced information security management and monitoring. Before working in the private sector, Mr. Yoran was the Director of the Vulnerability Assessment Program within the Computer Emergency Response Team at the Department of Defense and the Network Security Manager at the Department of Defense where he was responsible for maintaining operations of the Pentagon's network. Mr. Yoran has a B.S. from the United States Military Academy at West Point and an M.S. from George Washington University.

Legal Insights *(Cont. from Page 8)*

Intercept and Obstruct Terrorism, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[iii] The Act at Section 216. This is an enhancement to an existing statute that permits installation of devices to record pen register (digits) and trap and trace (incoming/outgoing calls.) These are constitutional under an expectation of privacy analysis - *see Smith v. Maryland*, 442 U.S. 735 (1979). Section 216 modified 18 U.S.C. § 1323 (a)(1) (2003). Prior to the Act, whenever a suspect moved to another jurisdiction and acquired another phone, a separate PR/TT had to be applied for.

[iv] 84 Geo. L.J. 2381 (1996).

[v] *Sidis v. F.R. Publishing*, 113 F.2d 806 (2d Cir. 1940).

[vi] *Sipple v. Chronicle Publishing Co.*, 201 Cal. Rptr. 665 (Ct. App. 1984)

[vii] *See Los Angeles v. Lyons*, 461 U.S. 95 (1983) (Injunction against L.A.P.D. use of chokeholds denied as the complainant, Lyons had no standing.) *But see*, 42 U.S.C. 14141, establishing causes of action for systematic, governmental abuse of Constitutional rights. See also *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*, 403 U.S. 388 (1971) (creating a cause of action against government agents that violate Constitutional rights.)

[viii] *See Katz v. United States*, 389 U.S. 347 (1967)(defining the modern objective standard defining the need for a warrant to search wherever the individual has "a reasonable expectation of privacy.")

[ix] The refinement of this approach to PR/TT's derived largely from discussions with Professor Jeffrey S. Parker, Dean Winton S. Moore, and Mrs. Tecla Murphy. Any misstatement remains mine. ❖

Noftsinger *(Cont. from Page 9)*

defining their roles and working to build a trust relationship that will continue to lay a foundation for further work.

As the partnerships between government, private industry and academia grow and expand, we stand better prepared to face oncoming challenges. Together these groups can provide strategic coordination and insight into the federal research agenda that drives us forward and seeks answers to the questions central to our purpose. The coordination of these efforts would ensure that while problems are explored, research would not needlessly overlap and would not carelessly expose the information critical to protecting our critical infrastructures. Additionally, to improve the products and applications desired by owners and operators of infrastructure systems, a strong, cohesive federal research agenda would help set and drive the priorities of the many agencies, such as DHS, NSF, NIST and DOD that contribute to this progress. In pace with these research efforts, we must also continue to study legal and policy initiatives that ensure that technology can be implemented in an efficient and useful manner aligned with sound policy.

More than anything, as we look into this new year, it becomes abundantly clear that while each critical infrastructure sector is vastly different in the role that it performs and the needs it has, all are linked through an immense web of interdependencies. These interdependencies provide challenges, yet they serve to remind us that no one group can do this alone- it will require the effort, support and energy of everyone- and more importantly, we all have a vested interest in the outcome. Collaboration, partnership and coordination will continue to be our guiding principles as we move on to tackle a new year of unforeseen challenges and unimagined success. ❖

Functional Roles Assigned by HSPD-7	
Agency	**Function**
State Department	Coordinate with foreign countries on infrastructure protection
Department of Justice and Federal Bureau of Investigation	Investigate terrorist activities aimed at critical infrastructure
Department of Commerce	Work to improve technology for cyber systems
Office of Science and Technology Policy (Executive Office of the President)	Coordinate interagency infrastructure research and development
Critical Infrastructure Protection Policy Coordinating Committee (created by HSPD-7)	Advise DHS on interagency policy
Office of Management and Budget	Oversee implementation of policies, standards and guidelines for Federal government computer security programs
Chief Information Officer Council	Improve information resources
Department of Transportation	Collaborate on all transportation issues

The CIP Project is part of the National Center for Technology and Law at the George Mason University School of Law. It is a joint initiative between GMU and JMU that examines law, technology, and policy to find comprehensive solutions to the most pressing CIP issues for policy makers and critical infrastructure owners and operators. The CIP Project was launched in May 2002. The CIP Project encourages participation by representatives from all levels of government, academia, and private industry.

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Project. 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/archives/cipp-report-l.html.