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

Focus on Information Sharing

A Message from Director John McCarthy:

The CIP Project is making significant progress in engaging legal scholarship in the issues of cyber security and critical infrastructure protection. We have launched a series of legal symposia addressing CIP issues. Last month's symposium on Information Sharing is summarized in this newsletter. Future symposium topics range from open source software code to the legal implications of port security operations. Additionally, we have sponsored several scholars to develop legal precepts in the field of critical infrastructure.

The CIP Project has advanced the ball in developing new sources of funds and new project grants. We have received funding from the National Defense University (NDU) to look into infrastructure interdependencies and we received a grant from the Department of Energy (DOE) to perform a peer review assessment of the National Infrastructure Simulation and Analysis Center (NISAC) Program. The most exciting news, however, is that the CIP Project has received another $6.5 million in appropriations. This means that the work we have started will be given time to grow and to make a positive impact in protecting our nation's critical infrastructure.

This issue of *The CIP Report* focuses on information sharing. Since the earliest days of the President's Commission on Critical Infrastructure Protection, information sharing has been considered one of the pillars of CIP. Presidential Decision Directive-63 urged each sector to establish an Information Sharing and Analysis Center (ISAC) in order to analyze and disseminate threat and vulnerability information as quickly as possible to minimize loss. To date, there are 12 ISACs in operation. They are organized uniquely, and have experienced varying degrees of activity and success. But regardless of each ISAC's experience, information sharing has significantly enhanced the security of the entire global network.

This issue highlights several ISACs and information sharing organizations, and examines some of the issues inherent in information sharing. I hope that you find it informative and thought-provoking!
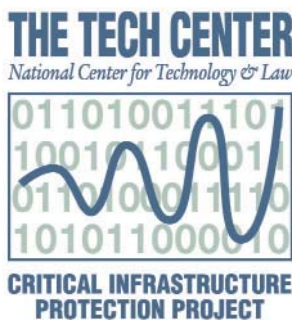
Making the Most of an Opportunity

by Stevan D. Mitchell

"Each American who depends on cyberspace, the network of information networks, must secure the part that they own or for which they are responsible."

-- The National Strategy to Secure Cyberspace (Feb. 2003)

The President's "National Strategy to Secure Cyberspace" (hereinafter ("National Strategy") contains this and numerous passages that are music to the ears of a veteran of the "infrastructure protection" wars. Behind us for now are the inevitable biproducts of earlythink -- paternalistic exhortations that government (much less any single agency) can meaningfully accomplish so large a task for others.

But with liberation comes responsibility, and with responsibility will come accountability. Because of the dependencies that have arisen and interdependencies we share through reliance on the 'net, those who fail to carry their burden will be singled out for their shortfalls - and interventionist remediation could easily follow.

The private sector has been given an opportunity to demonstrate that it can look after its own more efficiently and more appropriately than through government-centric or regulatory approaches. It has been given a reprieve, but must show it can follow through on the expectations held out for it.

An area in which expectations have been articulated with greatest clarity is information sharing. The National Strategy highlights the importance of information sharing and analysis and the expectations the federal government has for institutions that have already begun to step up, within discrete infrastructure sec-

Stevan Mitchell served as a Commisioner of the President's Commission on Critical Infrastructure Protection from 1996 - 1998. He is now Vice President of Intellectual Property Policy for the Interactive Digital Software Association.

tors, to take on the operational challenge -- sectoral Information Sharing and Analysis Centers (ISACs).

It is commendable that the Strategy recognizes both the importance of information sharing and the indispensable role played by the private sector in it.

Civilian targets are fair game. Private networks are vast, target-rich environments. The most effective detection strategies are the most highly decentralized insofar as they can be everywhere at once.

Motivated private sector participation is an essential element of a national strategy, and to be effective it must be nurtured - not compelled. The strategy rings the proper tone of deference, and suggests a willingness to accept an appropriately arm's length relationship with ISACs and their participants.

On the other hand, it is an arm's length relationship laden with obvious and specific expectations. The Strategy acknowledges the traditional role that many ISACs have come to fill vis-a-vis their respective infrastructure sectors:

Several sectors have formed Information Sharing and Analysis Centers (ISACs) to monitor for cyber attacks directed against their respective infrastructures. ISACs are also a vehicle for sharing information about attack trends, vulnerabilities, and best practices. *National Strategy at 8*.

(Continued Page 3)

(Opportunity continued)
"The federal government encourages the private sector to continue to establish ISACs and, further, to enhance the analytical capabilities of existing ISACs." *National Strategy at 21*.

But the Strategy also envisions ISACs as pivotal to tremendously broad array of assurance functions, some of which do not necessarily coincide with the core competencies that are being developed within these organizations, and many of which could contribute to costs.

The Strategy would also have ISACs:

• Provide representation for its constituencies in the "National Cyberspace Security Response System" *National Strategy at 20*;

• Serve as linkage to the Department of Homeland Security's "Incident Operations Center" *National Strategy at 21*;

• Share a role in the Department of Homeland Security's contingency planning efforts *National Strategy at 21*;

• Assist the Department of Homeland Security in the development of strong tactical and strategic analytic capabilities *National Strategy at 22*;

• Provide potential linkage to the government's "Cyber Warning and Information Network (CWIN)" *National Strategy at 23*.

The Strategy commends ISACs to corporations generally, as well as to colleges and universities. (*See National Strategy at 25, 41*). ISACs provide the spine for one of the very few courses charted in the Strategy for interfacing with State and local governments. *National Strategy at 48*.

While many expectations are recited, there is precious little articulated by way of direct support to ISACs that would allow then to grow, thrive and otherwise live up to these formidable expectations. These are, after all, voluntary organizations in their infancy, and even with narrowly focused objectives have proven relatively costly to maintain.

But no funding mechanisms, direct or indirect, are articulated for ISACs. There are no measures articulated to further incentivise ISAC participation - though it is certainly possible to think of a few. And there appears to be only a lukewarm commitment to seeking out and resolving both perceived and actual barriers that serve as impediments to public-private information sharing.

And at the same time that ISACs are given so pivotal an opportunity, participants should also consider the heavy burden the Administration would have them bear. This should be a time of reflection and decision-making along dimensions including functionality, participation, growth and governance, lest ISACs risk disappointing those who so clearly hold such high expectations for them. ❖
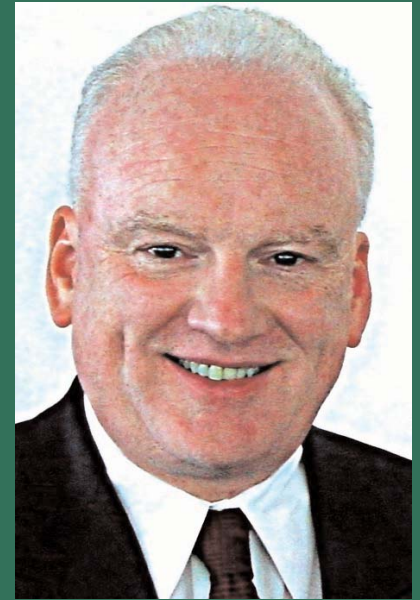
Richard A. Clarke, whose name is synonymous with Critical Infrastructure Protection, has resigned from his position as Special Advisor to the President for Cyberspace Security. Clarke's departure comes just after the release of the *National Strategy to Secure Cyberspace.*

Clarke began his federal career in 1973 in the Office of the Secretary of Defense. He later served at the Department of State, and has been at the White House for the last 11 years.

Clarke was a strong proponent of information sharing and public / private cooperation as a means of protecting the nation's critical infrastructure.

The CIP Project expresses its gratitude for Mr. Clarke's determined efforts to garner interest and action within the private sector, academia, Congress, and state, local, and Federal government. He will be missed.

Fire / EMS Sector ISAC Working with Nation's First Responders

Although Presidential Decision Directive 63 (PDD-63) identified Emergency Services as a critical infrastructure back in 1998, the events of 9/11 proved beyond the shadow of a doubt the absolute criticality of the nation's local fire and emergency medical departments-the first responders to any disaster, large or small. For this sector, firefighters, emergency medical technicians, and paramedics are the most important resource. But without their stations, apparatus, equipment,

communication systems, 9-1-1 systems, including immediate access to water, major roadways, bridges, and tunnels, it would be very difficult to fulfill their mission.

The U.S. Fire Administration (USFA) component of FEMA took on the responsibility of initiating a critical infrastructure protection (CIP) program to protect all of these assets after FEMA was named as the sector lead by PDD-63. The USFA formed the

Critical Infrastructure Protection Information Center (CIPIC), which has taken a very proactive approach to the task of serving as an information hub for all CIP matters in the Emergency Services sector.

In May of 2002 the USFA signed an agreement with the National Infrastructure Protection Center (NIPC) to establish the Information Sharing and Analysis Center (ISAC) for the Fire / EMS

ISAC	Operating Organization	Web Address
Banking & Finance (Financial Services)	LLC, Predictive Systems Inc.	http://fsisac.com/
Chemicals Industry	American Chemistry Council / Chemical Transportation Emergency Center	http://chemicalisac.chemtrec.com/
Electric Power	North American Electric Reliability Council	http://www.nerc.com/~filez/ cipfiles.html
Emergency Fire Services	U.S. Fire Administration	http://www.usfa.fema.gov/dhtml /fire-service/cipc.cfm
Emergency Law Enforcement	Independent organizations / Critical Infrastructure Protection Plan	http://www.nipc.gov/infosharing/ infosharing5.htm
Food	Food Marketing Institute	http://www.fmi.org/isac/
Information Technology	LLC, Internet Security Systems	https://www.it-isac.org/
Interstate	National Association of State CIOs	https://www.nascio.org/hotIssues/hs/index.cfm
Oil & Gas	LLC, Predictive Systems Inc.	http://www.energyisac.com
Surface Transportation	American Association of Railroads LLC/EWA	http://www.surface transportationisac.org/
Telecommunications	National Communications System/ National Coordinating Center for Telecom	http://www.ncs.gov/ncc/main.html
Water Supply	Association of Metropolitan Water Agencies	http://www.amwa.net/isac/

(Fire / EMS Continued) Sector in order to allow vital security-related information to move effectively between the Federal government and the national fire associations, the 50 State Fire Marshals, and the over 32,000 local fire and emergency medical departments throughout the nation. The ISAC is operated by the CIPIC at USFA headquarters in Emmitsburg, MD. The focus of the ISAC is to build an information sharing program that will make a difference in regards to survivability, continuity of operations, and mission success of the sector.

This ISAC is unique in that all fire and emergency medical personnel-both career and volunteer (which account for 75% of personnel)-are automatically members of the ISAC. This includes many departments that do not have subscriptions to sector periodicals in which the ISAC is publicized, or Internet access by which to learn about the ISAC. The CIPIC considers the difficulty of reaching all members one of its primary hurdles, and is aggressively working to meet the challenge.

One of the ways the CIPIC communicates with ISAC members is through the publication of weekly INFOGRAMs, which report news and information concerning the protection of the sector's critical infrastructures. INFOGRAMs report on a full range of issues affecting the sector, particularly threats that are deliberate (i.e.,

man-made), natural (i.e., wild-fires), or accidental (i.e., train derailment). Current and archived issues of the INFOGRAM can be found at http://www.usfa.fema.gov/dhtml/fire-service/cipc-info-grams.cfm.

The ISAC has also developed a Job Aid for its members, which is a guide to assist leaders of the fire and EMS community with the process of critical infrastructure protection. The document provides a model process for the systematic implementation of a CIP program that can be easily adopted by any local department or organization. The Job Aid contains a five-step process for CIP, but the methodology is supported by a philosophy that recognizes the importance of leadership buy-in and involvement, the prudent allocation of scarce resources, and the positive effect that a strong CIP program can have on both the sector and the communities that the sector supports.

The tools for communicating with the sector are evolving. A recent agreement between the USFA and the NIPC was made for interim use of the National Law Enforcement Telecommunication System (NLETS), a sophisticated message-switching network linking local, State, and Federal agencies together for the expeditious exchange of interstate law enforcement and public safety related information. The recent elevation of the Homeland Security Advisory System to "high" was communicated expeditiously to all law enforcement units via the NLETS system. But for the

first time ever, the message contained a header advising law enforcement units to disseminate the information to the department chief of their local fire and EMS organizations.

The ISAC's use of NLETS is a temporary arrangement until the sector has its own messaging system, which is expected to take the form of two separate list servers. One list server will be dedicated to disseminating sensitive but unclassified information to fire and EMS department chiefs. The other list server will be available to everyone in the sector-as well as law enforcement officers, emergency managers, and others who may benefit-for the dissemination of INFOGRAMs and other information that will be helpful in protecting the sector.

Perhaps the strongest asset the CIPIC has for information sharing is a close relationship with the NIPC, which has an Emergency Services sector representative on staff. To maximize the benefits that this relationship affords, the CIPIC urges sector members to report any and all suspicious activity, and certainly any criminal activity such as theft of emergency vehicles. Something may seem innocuous at the local level, but mapped with other reports at the NIPC can reveal a pattern that the sector needs to know about. The CIPIC does serve as the conduit for information sharing between the sector and the Federal government (via the NIPC) but urges sector members to report any urgent or imminent threat information directly to the NIPC. ❖

LEGAL INSIGHTS

by Emily Frye

Information-Sharing Hangups: Is Antitrust Just a Cover?

Sharing information about cyber-vulnerability, and responding effectively to such information, is essential to protecting critical infrastructures. Fear of antitrust liability has long been cited as an obstacle to sharing information about cyber-vulnerability. Consequently, fear of antitrust liability is also cited as an obstacle to building Information Sharing and Analysis Centers (ISACs) for each of the critical functions that is housed primarily in the private sector. This oft-referenced deterrent was the primary reason that the CIP Project sponsored "Information Sharing and Antitrust: Identifying Issues, Creating Solutions" on January 30.

There appears to be a narrow subset of circumstances under which antitrust liability might attach to information-sharing activities: when an industry seeks and obtains a Business Review Letter from the Department of Justice, for instance, and subsequently takes action that exceeds the scope of comfort provided by the DoJ. Other hypotheticals could be devised, surely.

But the largest obstacles to information sharing have nothing to do with antitrust. They are, instead, more complex and far less law-oriented. First and foremost, the perception that antitrust liability may attach to ISAC activity deters maximal - or even reasonable - information

sharing in some sectors. Industry participants may not fear regulators, from whom they can obtain business review letters and with whom they can build relationships. Certainly, however, they fear the possibility that unknown third parties will sue them.

Third parties may sue them for antitrust or anticompetitive

> *Information sharing, in its most effective form, stems from trust. And trust cannot be imposed by regulation, by exhortation to patriotism, or by membership in an ISAC.*

behavior, due to any number of motivations. One of the possibilities that ISACs are concerned about is the situation in which a product-based vulnerability becomes apparent that pervades (or threatens to pervade) an entire industry. One of the members of the ISAC believes that it has determined the source of the problem; in an effort to protect the entire industry, the member circulates a warning. The industry as a whole then ceases to use or purchase the product. The producer of the defective product is angered by the lost sales, and sues on anticompetitive-behavior grounds. Even if the ISAC mem-

bers win - and, under these facts, they probably would - lawsuits are tremendously expensive in both time and money. As Symposium speaker John Burke put it, it is not enough to tell a group of powerful CEOs that "we might not have a problem."

Second, and far more subtle, the mask of antitrust can serve as a convenient (even polite) excuse for the truth: information sharing, in its most effective form, stems from trust. And trust cannot be imposed by regulation, by exhortation to patriotism, or by membership in an ISAC. Trust can only be … "nurtured," if you will.

If lack of trust is the problem, as well it might be among competitors, then the solution is not Congressional antitrust protection for ISACs. Nor is it likely to be command-and-control regulation, because the private sector knows its challenges better than regulators; the private sector can react more immediately and efficiently - given the motivation to do so. What is, then, the motivation to increase vigilance, to protect networked systems, and to share information detected? The private sector operates on economic incentives. They will only engage in such societally optimal behavior if they derive an economic benefit from doing so. Can the law and policy community do a better job of defining economic benefits for ISAC development?
(Continued Page 7)

(Legal Insights Continued)

Perhaps, in the end, the solution will come from adapting the methods of economist Ronald Coase to the newer challenge of cybersecurity: flip the problem on its head. Ask, instead, what are the legal and economic consequences of not sharing information? Within the past month, an Internet worm has disabled ATMs, a class-action lawsuit has been filed over a network-security breach leading to data-privacy infringement, and both the Bush Administration and the European Union have announced that they are formulating plans for cyber-warfare. None of these events were specifically anticipated by the private sector. The case for information-sharing becomes stronger as the economic uncertainties of the networked world expand; the case grows incre-

mentally stronger over time. Take the next step: pacemakers are moving toward online man-

Emily Frye, CIP Project Associate Director, Legal Programs

agement systems. Consider the situation in which one or more of the manufacturers is aware of a security flaw in the system, but does not share the informa-

tion. A malicious actor hacks the system, causing heart attacks and death. The lawsuits from the affected parties would make antitrust appear irrelevant.

Making allies of competitors may take a miracle, but surely it requires a clear demonstration of necessity. Educating the key decision makers, such as General Counsels and Chief Executive Officers, about the very real threat associated with failure to communicate is an important part of increasing the effectiveness of information sharing. Legal scholars can support the effort by pinpointing and articulating the benefits of information sharing. The Academy offers no miracles. But education is indeed on offer. ❖

Internet Security Alliance: Building on Experience to Enhance Security

The Internet Security Alliance (ISAlliance) is a public-private partner-ship that provides its participants a mutually beneficial forum for information sharing and e-security issues. It is an industry voice that advocates practical and effective solutions to information security and critical infrastructure issues. Within ISAlliance, industry leaders share invaluable insight stemming from their experiences tackling a wide range of information security problems. ISAlliance members are cross-sector and international in nature. What binds them together is a commitment to improving the security of their information systems. The ISAlliance encourages its partici-

pants to implement a host of best practices in network security and infrastructure survivability. The forum seeks to foster a collaborative environment in which the sharing of time-sensitive information leads to security solutions that are easier to understand and implement. Above and beyond this, ISAlliance articulates the industry's concerns on Capitol Hill.

ISAlliance is a collaborative effort that has included the leaders of the information security field from the beginning. These include Carnegie Mellon University's Software Engineering Institute (SEI), the CERT® Coordination Center (CERT/CC), and the Electronic Industries Alliance (EIA), a federation trade associations

representing 2,500 companies. The forum that they have created allows its participants to access up-to-the-minute threat reports, learn of best security practices, and discuss valuable risk management strategies. The goal is to give them an edge in the highly competitive and uncertain environment of the Internet by protecting their information systems from the dangers that are inherent in connecting to the Internet. Best of all, ISAlliance members are able to access all of this via a single Internet portal.

What makes an initiative on this scale possible is the enormous amount of data that is available to *(Continued Page 8)*

Collaboration on Computer Security at the CERT / CC

One of the oldest and most unique information sharing organizations, CERT® Coordination Center (CERT/CC) serves as a center of Internet security expertise and shares a wide range of computer security information with a broad audience of government and private sector organizations. The work of CERT/CC is premised on a model of information sharing in which collaboration with the Internet community is critical to detecting and resolving computer security incidents and preventing future incidents. CERT/CC's mission concentrates on providing a comprehensive view of cyber attack methods, vulnerabilities and the impact of cyber attacks on information systems and networks, as well as providing methods to evaluate, improve and maintain the security and survivability of networked systems.

CERT/CC is located at the Software Engineering Institute (SEI), a federally funded research and development center operated by Carnegie Mellon University. CERT/CC was created in response to the Morris worm incident in November of 1988, which halted about 10 percent of all Internet systems. At that time, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies as well as to help mitigate the occurrence of future incidents.

Since its creation in the late 80's,

CERT/CC has been working to fulfill its initial tasking and has helped to establish other response teams as well as incident handling practices that have been adopted by more than 200 response teams around the world. Today, CERT/CC continues to respond to security incidents and analyze product vulnerabilities, but as the global dependence on networked systems and the Internet has grown, so too has the center's role.

To better manage the new dependencies and changes in systems security, CERT/CC is now part of the larger SEI Networked Systems Survivability Program. The primary goals of the program are to ensure that appropriate technology and systems management practices are used to resist attacks on network systems; and, to limit damage and ensure continuity of critical services when successful attacks do occur. CERT/CC focuses their work in the following key areas in order to meet these goals: survivable enterprise management, survivable network technology, incident handling and analysis, vulnerability analysis, and education and training. Additionally, CERT/CC collects and disseminates information through multiple channels in order to increase awareness of security issues and help organizations improve the security of their systems.

Together with the Electronic Industries Alliance (EIA), a federation of trade associations, and the SEI, CERT/CC formed the

Internet Security Alliance. It was created to provide a forum for information sharing and thought leadership on information security issues. It provides members with a single portal for up-to-the-minute threat reports, best security practices, and risk management strategies, among other things. The ISA aims to cut across industries and market sectors to develop a global approach to the problems inherent in electronic commerce and communications. Most recently, ISA released the "Common Sense Guide for Home and Individual Users", a primer on basic cyber-hygiene. ❖

(*ISAlliance Continued*) the CERT/CC. It is the world's preeminent authority for information security research. Furthermore, the analytical expertise found at the CERT® Analysis Center draws on lessons learned from both the public and private sectors. The Analysis Center's insight and instruction is available for the benefit of all alliance members.

Within ISAlliance, companies are empowered not only to participate in the information security debate, but, more importantly, to help implement solutions. ISAlliance members also take pride in the fact that they are not only helping to improve the security and survivability of their own networks, but also to improve the security and survivability of the Internet itself. Best security practices are identified, developed, documented, and matured. They will help all members to combat evolving Internet security threats well into the future. ❖

Telecommunications ISAC

In January 2000, the National Coordinator for Security, Infrastructure Protection, and Counterterrorism designated the NCC-ISAC as the ISAC for telecommunications. On March 1, 2000, the NCC-ISAC commenced operations. The initial NCC-ISAC membership is based on NCC membership, which is evolving to reflect a broader base of technologies comprising the telecommunications infrastructure.

NCC-ISAC will support the mission assigned by Executive Order 12472 and the national critical infrastructure protection goals of government and industry. The NCC-ISAC will facilitate voluntary collaboration and information sharing among its participants gathering information on vulnerabilities, threats, intrusions, and anomalies from telecommunications industry, government, and other sources.

The NCC-ISAC will analyze the data with the goal of averting or mitigating impact upon the telecommunications infrastructure. Additionally, data will be used to establish baseline statistics and patterns and maintained to provide a library of historical data. Results will be sanitized and disseminated in accordance with sharing agreements established for that purpose by the NCC-ISAC participants.

Building a Next Generation ISAC in the Financial Services Sector

The Financial Services ISAC (FS-ISAC) is building a "next generation" ISAC-expanding its current scope and membership to benefit the entire sector with broader analysis of threats and vulnerabilities. When the FS-ISAC opened for business in 1999, it became the first private sector ISAC. Since then, the ISAC has grown in both size and capabilities to assist the banking and finance sector (collectively holding about $21 trillion of the U.S. financial sector's assets).

The ISAC's primary value is in its ability to quickly alert members to potential security threats and to act as a repository for information specific to the financial services community. Much of the information disseminated by the FS-ISAC can be obtained from other sources, but putting it all together would be a time-consuming process for any single company. The ISAC provides a one-stop-shop for vulnerability, threat, incident, and response information.

ISAC members, who remain completely anonymous, have a choice in how they receive information from the ISAC-it can be accessed on secure members-only sections of the website, or can be disseminated by pager, fax, e-mail or phone. The group also holds two meetings each year. Any report members share with the ISAC is scrubbed of sensitive proprietary information. Each report is analyzed by security experts at Global Integrity, who operates the ISAC, before being disseminated to the broader group. Security alerts are given a rating from informational to crisis mode.

Major banks, brokerage houses and insurance companies make up the bulk of membership, but the next generation model that the ISAC is building includes financial service associations, which were previously not allowed to join.

The financial services sector has shown great leadership in information sharing and other CIP efforts. Watch in the coming months as the sector develops a new model for information sharing that is likely to be emulated in other sectors. ❖

Information Sharing and Antitrust: Identifying Issues, Creating Solutions

On January 30th, the CIP Project kicked off its conference series with "Information Sharing and Antitrust: Identifying Issues, Creating Solutions", a symposium on antitrust impediments facing Information Sharing & Analysis Centers (ISACs). Held at the George Mason University (GMU), the CIP Project welcomed thought-leaders, government and industry practitioners, and academicians to discuss antitrust issues in the context of ISACs and critical infrastructure protection. The event was educational and informative, as expert speakers and panelists raised varying views in their exploration of the issues.

The symposium began with opening remarks from GMU Law School Dean Mark Grady and an introduction to the CIP Project and the day's events by Executive Director John McCarthy. John Marsh, Former Congressman and Secretary of the Army, discussed the origins of the critical infrastructure protection movement. He sees a significant role for lawyers in the dialogue, and spoke about Congress' adaptability and potential for dealing with antitrust laws in the context of ISACs. Dean Mark Grady was next on the agenda, and he raised the importance of private industry solutions to address the legal impediments facing ISACs. Dean Grady presented the view that antitrust issues are not necessarily an impediment to ISACs and suggested that ISACs could evolve into a cooperative system - he looks to non-traditional solutions to resolve issues.

Former Director of the Critical Infrastructure Assurance Office (CIAO), John Tritak, provided his perspective on the concept of information sharing in critical infrastructure protection and the evolution of ISACs. Mr. Tritak stated, "Industry talks about the liability of information sharing and the legal impediments, but they don't talk about the liability of not sharing," stressing the importance of information sharing and highlighting the potential challenges ahead.

Wrapping up the morning session, Alden Abbott, Assistant Director for Public Policy and Evaluation in the Bureau of Competition at the Federal Trade Commission (FTC), provided the FTC's perspective on information sharing and antitrust. "Properly structured, there should be no problem with anti-trust and information exchanges," he stated as he began his discussion. Mr. Abbott distinguished the government's historic perspective on information sharing as anti-com-

petitive behavior with its current consumer-focused perspective that views information sharing positively. Additionally, he stressed the importance of the business review letter for ISACs.

Lunch provided a short break, as well as an opportunity for participants and speakers to mingle and review the morning's presentations. Moderator Amitai Aviram, Visiting Assistant Professor at GMU Law School, then set the tone for the afternoon panel, "Perspectives on the Antitrust Issue." Panelists included Steven Chabinsky, Assistant General Counsel to the FBI and Principal Legal Advisor to the National Infrastructure Protection Center (NIPC); Stevan Mitchell, Vice President of Intellectual Property Policy for the Interactive Digital Software Association and former Commissioner of the President's Commission on Critical Infrastructure Protection; John

John Burke, General Counsel, BITS

Food Industry Playing Role in CIP

On February 15, 2002, Food Marketing Institute (FMI) President and CEO Tim Hammonds and and the Director of the National Infrastructure Protection Center (NIPC) signed an agreement establishing a public/private sector partnership with the Food Industry Information Sharing and Analysis Center (ISAC) led by FMI. The Food Industry ISAC has a threefold mission:

iTo provide information and analysis services that will enable the food industry to report, identify and reduce its vulnerabilities to malicious attack and to recover from any attacks as quickly as possible.

iTo work directly with the NIPC and the FBI's Weapons of Mass Destruction Unit to identify credible threats and craft specific warning messages for the food industry.

iTo facilitate the development of, and serve as a central repository for, best practice recommendations and countermeasures for preventing and recovering from malicious attacks. These would include bioterrorism attacks,

"In the wake of September 11 all of America's strategic industries are now on the front lines of the war on terrorism."

Tim Hammonds President and CEO Food Marketing Institute

attacks on physical assets, and cyber attacks on the industry's computer or financial networks.

FMI has a long history of working with the FBI and other law enforcement agencies, including successful programs to combat in-store bank robberies, apprehend professional check forgers, rescue missing children, and combat organized retail theft rings.

Ron Dick, former director of the NIPC, explained why FMI is positioned to be a natural leader for the Food Industry ISAC: "The food industry is so large and diverse that there are literally thousands of contact points. But the entire industry comes together in the supermarket. That makes FMI a logical organization to coordinate an industry-wide effort."

Because the food supply is a critical national resource, the Food Industry ISAC is supported by FMI at no additional charge to those food industry companies that participate. ❖

(ISAC Symposium Continued)
Burke, General Counsel to BITS (the technology group of the Financial Services Roundtable); Louise Tucker, Senior Counsel to Telcordia Technologies and Chair of the Legal and Regulatory Group with the National Security Telecommunications Advisory Committee; and, Dean Mark Grady.

Each panelist brought a unique perspective to the discussion about ISACs and antitrust, providing insightful comments on the topic. Mr. Chabinsky focused on some areas where industry has not made a strong enough case to induce government to take action with relation to the antitrust issue. Mr. Mitchell talked about the future of ISAC governance and interconnection and how a new ISAC paradigm "may impact the antitrust issue down the road." The issue of liabilities and industry's insecurity about antitrust was raised by Mr. Burke's remarks. Ms. Tucker related the experience of the Telecom ISAC with regard to antitrust and other legal issues. Finally, Dean Grady stressed the lack of financial incentives as the reason for reduced engagement in ISACs. These varying points of view generated a brief but lively discussion, concluding the afternoon panel.

The CIP Project anticipates that the success of the ISAC Symposium presages an ongoing series of dynamic events on relevant topics in critical infrastructure protection. ❖

UNIVERSITIES UNITE FOR COMPUTER SECURITY

by Taz Daughtrey

Computers are the key infrastructure element for data management and communication on the college campus, and the user community is probably as diverse in its skills and care as anywhere.

The University of Virginia, Virginia Tech, James Madison University, and George Mason University are pooling their resources to strengthen computer security programs throughout Virginia higher education. The "Virginia Alliance for Secure Computing and Networking" will do so by integrating and making available field-proven tools, best practices, and people from the Alliance's partner institutions.

Formed in response to, among other influences, the charge given the state's two cyber-security research centers to assist in meeting Virginia government security goals, participants have been working together since this past summer. These participants include the representatives from the Critical Infrastructure Protection Project, JMU's Commonwealth Information Security Center, GMU's Center for Secure Information Systems, and security practitioners at UVA, Virginia Tech, JMU, and GMU.

The Alliance has been endorsed by the state's Higher Education CIOs Group and is targeting its first delivery of services and products by March 2003.

Offerings in preparation include:
- Security training courses
- Consulting on a variety of security topics
- Web-based toolkit of security tools and best practices
- "Ask the expert" email service
- Moderated mail list for general security discussions
- Periodic information sharing meetings and workshops
- Expansion and promotion of existing higher education VA-CIRT group for inci   dent alerts and reporting
- Comprehensive secure university model responsive to Commonwealth and Federal security regulations and guidelines.

These products and services are being developed as generically as possible so they might be expanded to use in state and local government agencies.

CIP Project Featured in Briefing to Virginia Research and Technology Advisory Commission

by Ken Newbold

ohn McCarthy, Executive Director of the CIP Project, and Dr. A. Jerry Benson, Dean of the College of Integrated Science and Technology at James Madison University, presented the CIP Project to the Virginia Research and Technology Advisory Commission (VRTAC). The briefing highlighted the research underway at George Mason University and James Madison University and outlined the future goals of the CIP Project.

As mentioned in the presentation, close ties between the CIP Project and VRTAC's goals can be seen. The CIP Project spans the research spectrum from basic theoretical research in cyber systems and economics to applied research in modeling and simulation tools to solve critical infrastructure problems. VRTAC and the CIP Project undertake studies to identify technologies, economic processes, and legal reforms and policy recommendations for core business functions.

Opportunities exist for VRTAC and the CIP Project to work collectively to advance Virginia's efforts in homeland security and critical infrastructure protection. The CIP Project is one of Virginia's flagship research programs underway in the area of homeland security. One such partnership opportunity is the Center for Innovative Technology's proposed Institute for Defense and

Homeland Security (IDHS). Virginia is home to many federal agencies, defense contractors, and world-class research universities which are all working in the area of homeland security. The IDHS proposes to bring higher education, private industry, and government together to bring time efficient solutions to practice in the nation's homeland security efforts.

VRTAC is a 29-member panel that was created to advise the Governor on appropriate research and technology strategies for the Commonwealth with emphasis on policy recommendations that will enhance the global competitive advantage of research institutions, not-for-profit research capability and technology-based commercial endeavors within the Commonwealth. The commission is co-chaired by Mr. John Backus of Draper-Atlantic and Dr. John Noftsinger of JMU. Dr. Noftsinger serves as Principal-Investigator of the Critical Infrastructure Protection grant at JMU.

Virginia's research agenda was presented to the Commonwealth's Congressional delegation on Capitol Hill Day, which was held February 5th, and was extremely well received for its focus and relevancy. As seen by VRTAC, growth areas for Virginia include: biotechnology, information security, nanotechnology, sensors, and wireless communication. ❖

Information Sharing in the Energy Sector

With an increased dependence on advanced information systems for efficient energy generation, transmission, and distribution, the oil and gas sector's vulnerability to physical and cyber
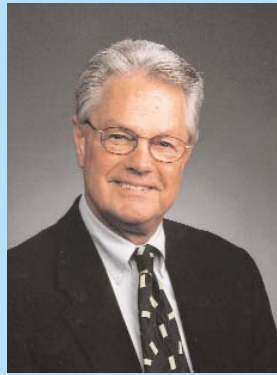
Bobby R. Gilliam Manager of Global Security, ConocoPhillips, Inc., Chair, Energy ISAC Board of Trustees

attack has grown over the past several years. In order to address this vulnerability, the sector created the Energy ISAC in November of 2001, complementing the Electric Power ISAC which was established about a year earlier.

The vision of the Energy ISAC is to provide a unique and customized set of information sharing and analysis services that will enhance the capability of the energy industries to identify and reduce infrastructure vulnerabilities, to protect from cyber or physical attacks or disruptions, and to respond to and recover from attacks or disruptions restoring service to customers as quickly as possible.

Some of the services provided by the Energy ISAC include:

• Clearinghouse for security information including warnings and other information from the National Information Protection Center

• Near real-time warnings of potential threats on a 24/7 basis

• Identification of vulnerabilities from both cyber and physical threats

• Professional analysis of threats at the micro and macro level

• Security solutions and patches, and access to Best Practices information

• A secure and trusted means of communication between members

• Sector specific information such as SCADA vulnerabilities, physical threat data specific to the industry, and threat conditions as reported by sector-related agencies

Though information is gathered from a wide range of sources, including members, the government, other industry ISACs, and other sources, the Energy ISAC ensures that the information stays within the ISAC.

Government agencies may submit data to the ISAC, but may not access any information from the ISAC. The Board of Managers must approve any sharing of ISAC information with outside entities. This policy creates a trusted and secure environment for members.

The Energy ISAC is a key player in CIP efforts, and has succeeded in reducing its sector's risk and exposure to threat and vulnerabilities through early warning, event analysis, and information sharing expertise. ❖

FedCIRC Requests Industry Collaboration on Security Standards

Charged with serving the government community in meeting computer security challenges, the Federal Computer Incident Response Center (FedCIRC) is the central hub for all Federal civilian agencies and departments sharing computer security information. The FedCIRC provides a government-wide approach to computer incident response handling as well as a mechanism through which vulnerability and incident data may be shared. The FedCIRC brings together a collaborative partnership of common security and incident response elements within the Federal government, law enforcement, academia, and private industry to jointly address threats to the critical information infrastructure, ensuring that the Federal government's critical services can withstand or quickly recover from possible attacks on its information systems and resources.

FedCIRC services can be categorized into several discreet offerings, each of which reflects the collection, analysis, and assessment of security and risk data. FedCIRC Services include:

• Provides analysis of computer security issues, trends, and risks - including occurrences, threats and vulnerabilities.

(FedCIRC continued)

• Offers an information security snapshot.

• Offers corrective actions and options.

• Provides 24/7 Support

• Offers the Patch Authentication and Dissemination Capability, which is a new web-enabled service for providing validated patches and notifications on new threats and vulnerabilities

FedCIRC's most valuable offering is in coordinating information and services within the Federal civilian community. Federal civilian agencies require various support for addressing computer security and risk management challenges. Coordination involves not only presenting a clearly defined, single point of contact, but also a trusted broker that translates computer security issues across the entire community.

For some time, FedCIRC has been collaborating with the CERT Coordination Center (CERT/CC) on a solution for analyzing and

correlating computer security incident information across the government. The program is called the Data Analysis Capability (DAC). Agencies have already tested the DAC and faced difficulty merging information from different commercial

intrusion detection and management systems.

In early February 2003 FedCIRC issued a request for information (RFI) asking industry to work with the CERT/CC and the Internet Engineering Task Force to develop common standards for exchanging security incident information, including the Intrusion Detection Message Exchange Format and the Incident Object Description and Exchange Format. Although these standards are independent from the DAC, the RFI states that "compliance with the DAC architecture is likely to become a requirement for future acquisition of security-related products by federal civilian agencies." The next round of testing of the DAC is planned for spring 2003. Responses to the RFI are due to FedCIRC by February 28 at dac-rfi@fedcirc.gov. ❖