JUNE 2003 / VOLUME 1, NUMBER 12

THE CIP REPORT

CIP PROJECT RESEARCH ISSUE

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*

Rebecca Luria, *CIP Project Administrator / Executive Assistant*

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

George Baker, *Associate Director, JMU Institute for Infrastructure and Information Assurance*

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

Contact: cipp01@gmu.edu
703.993.4840

Message from John McCarthy, Executive Director, CIP Project

This edition of the newsletter marks a significant milestone for *The CIP Report* - a year in publication. Since the Inaugural Edition in July of 2002, *The CIP Report* has strived to advance the dialogue between industry, government, and academic professionals with an interest in critical infrastructure protection. Focusing on individual industry sectors and important developments in critical infrastructure protection over the past year, *The CIP Report* has endeavored to be an interesting and informative tool.

It is my pleasure to provide this second special edition of *The CIP Report* that highlights the excellent work of the George Mason and James Madison scholars supporting the CIP Project. In this newsletter, we will present an overview of the ongoing and planned research activities of the CIP Project as well as some important events with which we have been involved. We will bring you up to speed on the progress of the research projects that were introduced to you in the October newsletter and have now begun to develop tangible solutions and results. We will also highlight the scope of our newly funded research projects that are currently getting underway.

In addition to the research projects, this newsletter will note several highly successful conferences that we have organized and hosted on topics ranging from ISACs and the impediments posed by antitrust laws, to the security implications of the use of open source and proprietary software, to legal questions at the forefront of national security. In particular, I would like to recognize the support of our distinguished Senior Fellow, Frank Sesno, for his contribution to the superb event we held at the National Press Club on June 18th. This event, which inaugurated our new series "CIP Critical Conversations", is another example of the CIP Project's commitment to bringing together government and industry leaders, legislators, and scholars to engage in a dialogue about key issues in critical infrastructure protection. We are looking forward to future such events.

I hope that this issue of *The CIP Report* is informative and useful and conveys our sense of pride in the work that the CIP Project has achieved.

The Virginia Institute for Defense and Homeland Security (IDHS) held a summit on June 25th showcasing cutting-edge defense and homeland security research from Virginia's universities in the areas of telecommunications, sensor systems, biodefense and risk management. In the keynote address opening the day's events, Virginia Governor Mark R. Warner gave special recognition to Secretary Jack Marsh for his efforts in the State of Virginia and stated that the Critical Infrastructure Protection Project is a "model of collaboration" in Virginia. (See Page 22 for more on the IDHS.)

Index of CIP Project Research Acitivities

Update on Academic Research Activities

Internet Infrastructure Study
Led by Laurie Schintler, GMU-Public Policy

Much of the effort to date has gone into developing a geo-spatial database of telecommunications infrastructure and other features such as critical financial services along with a set of analytical tools that can be used to explore and visualize the data to identify where potential vulnerabilities exist. These tools have been used to conduct analyses at the national level and the metropolitan regions of New York City and Washington, D.C. Parts of the analysis have been presented to the National Communications System, members of the Financial Services Roundtable and a variety of academic and trade meetings. As the project comes to a close, the team is beginning to focus attention on the next phase looking for partners and defining an agenda for further research in this area.

Attacker Fingerprinting and Identification
Led by Sushil Jajodia,GMU-IT&E

Researchers Sushil Jajodia and Ninging Wu are employing a series of data mining techniques including association rules, classification techniques, and pseudo-Bayes estimators to detect cyber attacks using the network audit trail data. Their technique is novel in two ways: first, it compares the suspicious rules with a previously generated profile of "normal" rules and selects only rules not in that profile. Second, the technique involves mining incrementally by sliding a time window over the audit trail data, as it is being generated. They have also produced a report, "Mining unexpected intrusions in network audit trails," to be published in the journal *Distributed and Parallel Databases.*

Economic Modeling of Cyber Security
Led by Vernon Smith, GMU-Interdisciplinary Center for Economic Science

The "Economic Modeling of Cyber Security" and "Security, Efficiency and Pricing Performance of Enhanced Electric Power Markets" are moving forward and continue to be refined. The faculty of the Interdisciplinary Center of Economic Science (ICES), under the general direction of Nobel Laureate Vernon Smith, are at the cutting edge of this critical research agenda. A network is only as secure as its least secure node. The research is an important step in creating new institutions that help to ensure each node chooses the optimal level of security, in view of both itself and the security of others on the network. Both theory *(Continued, Page 4)*

High Reliability Networks, Disaster Mitigation and the World Trade Center: Analysis of Technological, Organizational and Social Factors Affecting Performance of a Critical National Economic Concentration

This research has been focused on "drilling down" to exploit specific case material arising from the World Trade Center event of September 11th. Documentary data collections have been performed along with a series of oral interviews with individuals from key government and industry players involved in the reconstitution efforts post 9/11. Using these data along with insights gained through review of the existing and emerging scientific literature on emergency management, detailed policy recommendations and implications of national authority in re-establishing key crashed networks is being developed. These findings are directed towards the technological, organizational and human factors making up this economic concentration.

Secure University - Led by Ed Sibley, GMU-IT&E

Work so far on the "Secure University" has resulted in a 22 page, and growing, paper. The paper provides an overall discussion of the challenge of Homeland Security and the United States' efforts to meet that challenge. It further expands on the security needs of the state agencies in Virginia and ultimately discusses the role of security systems in universities. In the near term, the research team expects to articulate this work into a preliminary statement of the Strategic Requirements for Security in a University. The requirements will then be further expanded into a set of high level needs for the security of systems within universities. This will involve the security of material within universities, between universities, and from the universities to the state agencies with which they interact. Additionally, the CIP Project will fund Joy Hughes, CIO and Vice President for Information Technology at GMU, for a conference that will bring together university network security practitioners and university researchers to discuss and begin to close the gaps in university vulnerabilities.

Network Security Risk Assessment Model Tool, Led by Samuel Redwine, JMU-Computer Science

The James Madison University (JMU) CIPP research team aims to develop a Network Security Risk Assessment Model (NSRAM) Tool. This effort is driven by the need to predict and compute the probability of adverse effects that stem from system attacks and malfunctions, to understand their consequences, and to improve existing systems to minimize these consequences.

NSRAM is targeted at systems supporting critical infrastructures varying from individual systems to organization-wide systems, to systems covering entire geographical regions. Early work emphasizes computing systems, but systems sharing the network nature of computing systems, such as electrical and water supply systems are potential targets. Input consisting of network topologies and interdependencies, recovery and repair capabilities, attack scenarios, and traffic analysis data, will enable the NSRAM Tool to evaluate critical dependability issues including potential outage longevity and costs, data loss and those risks associated with network problems for user specified scenarios. Decision-making analysis support will be included to provide modeling to support design, operation, maintenance, continuity, and recovery of these systems.

It is expected that the initial products will be somewhat technical in nature for use by JMU consultant-level experts; however, immediate development work will concentrate on modeling computer security phenomena and user interface refinements to increase accessibility. At a minimum, the above requirements will be represented in a tool that meets the following baseline feature list:

- Extensible network and scenario modeling interface
- Network simulation engine
- Statistical analysis capability
- Report generation interface

To achieve this, work to date has involved the following:

- Problem domain research
- Network analysis and simulation tool investigation
- NSRAM requirements specification
- Initial prototype model development
- Initial prototype application development

The immediate future efforts of the JMU CIPP project are focused on the following three areas:

I. Augmentation of initial prototype

II. Analysis of a university computer network as the first client for the tool

III. Refinement of needs, features, and model and application designs

Use with the first client and the ongoing refinement mentioned in item three will in turn provide the direction for the production of future prototypes. Enhancement of features will be driven by modeling experiences with, and feedback from, JMU and other clients with the series of prototypes.

Smith *(Cont. from Page 3)* and experiments are in their early stages, but results to date are promising. The projects have progressed to the point where experiments using the proposed market pricing models have successfully been performed. Substantial progress has been made in understanding how a node's incentives for security are affected by important variables such as network size, number of network users, ease of security monitoring, and cost. In order to determine how to obtain optimum network protection, and using controlled laboratory experiments, the ICES team plays these and other variables against each other in a variety of different ways. The projects' combination of theory and experiment is the right way to analyze the economic complexities of cyber security.

A Comparative Analysis of Technological, Organizational and Human Factors Affecting Security in a Civilian & Military Network-Dependent Infrastructure Cluster: Crystal City and the Washington Navy Yard
Led by Todd LaPorte, GMU-School of Public Policy

This research focuses on examining, classifying and analyzing the differing dependencies for continued operation and disaster recovery of network-dependent infrastructures, including technological, organizational, jurisdictional and human factors. Comparisons of infrastructure vulnerability assessment processes and data gathering activities, vulnerability gap analysis, and sufficiency of risk management practices and policies have been ongoing. In addition, students participated in a practicum course and exercise evaluating methods of vulnerability assessment actions from local business owner perspectives. Work has been underway in categorizing factors effecting policies, regulations, and industry standards for collaborative management and governance of interdependent infrastructures. Continued emphasis has been placed on the basic premise - infrastructure protection involves "layered" defensive strategies that allow for graceful degradation of infrastructures and infrastructure interdependencies and toward that end actions to date include: development and assessment of an annotated bibliography of infrastructure and disaster management literature; assessment of network and infrastructure vulnerability data gathering methods and practices; identification and risk mitigation strategies for complex multiple network interdependencies, and identification and risk mitigation strategies for network failures and cascade effects. Final results of this research activity will be presented in the fall workshop, with policy recommendations and proposed actions for pre-emptive security.

National Infrastructure Simulation Analysis Center (NISAC) Peer Review for DHS
Led by Chris Hill, GMU-School of Public Policy


Chris Hill

For the Department of Homeland Security (DHS), George Mason University researchers, led by Principal Investigator Chris Hill and Project Manager Kip Thomas, reviewed the activities of the National Infrastructure Simulation and Analysis Center (NISAC). This assessment, or peer review, included both technical and strategic reviews as well as a written evaluation of the efficacy and sufficiency of NISAC.

The review effort focused on three interrelated aspects of NISAC and national critical infrastructure protection challenges: modeling, simulation, and analysis (MSA); management; and strategic direction. Through these lenses the project team examined the background of NISAC; the potential contributions of MSA to critical infrastructure protection; NISAC's contributions to critical infrastructure protection; and the quality of NISAC's programs, management and direction. With regard to MSA, the review provided an analysis of not only the ways in which MSA may add value to dealing with infrastructure protection challenges, but also the barriers, limitations, and problems associated with utilizing MSA in this arena.


Kevin Thomas

The study team's review resulted in nearly two dozen findings and recommendations on organizational structure, program management, and modeling activities. These conclusions will be used to help the Department of Homeland Security and NISAC raise the level and significance of their contribution to protecting the Nation's critical infrastructures.

Description of Newly Funded Academic Research Activities

Protecting the Nation's Blood Supply: A Critical Infrastructure
Led by Professor Arnauld Nicogossian, GMU-School of Public Policy

This study will address means for achieving a safer blood supply and blood products, by detecting organisms responsible for new and re-emerging infectious diseases and biological weapons. This study will evaluate available technologies for monitoring blood products as an early warning system for infections. This project will also establish a research and policy agenda that could lead to the deployment and operation of such a monitoring system (s). Early detection of infections might also help with the early diagnosis and treatment of chronic and debilitating illnesses such as cancer, arthritis and mental disorders.

A database is being developed that will help in designing accurate mathematical models of a potential bio-terrorist attack. To date, it has been decided that the contents of the database will include all known pathogens capable of transmission through blood components. Methods of detecting and monitoring the blood and blood products supply will be reviewed and reported. To establish the database, a comprehensive literature review is being conducted focusing on pathogens used as bio-weapons, infectious diseases transmitted through blood, and policy and politics of blood and blood products. A review of the current state of knowledge in modeling infectious disease transmission will be conducted by a selected group of experts in epidemiological models.

A Rights Based Solution to Critical Cyber Space Infrastructure
Led by Jack High and Bill Tulloh, GMU-School of Public Policy

This study will demonstrate that a general system of property rights will substantially reduce the threats now facing our nation's critical cyber space infrastructure. The study will show that a rights-based solution to cyberspace protection is practical, economical, and consistent with the norms of U.S. society.

The research will apply law and economic theory on two levels. The first level is the social realm, where the economic theory of property rights and spontaneous orders has been well developed, and where it is generally recognized that cyber security problems can be traced to the lack of well-defined property rights. The second level is the technical realm, consisting of the software code and protocols, where there is not general recognition that improper boundaries and ill-defined authority create vulnerabilities in our digital infrastructure. Further, the research will show that a solution to cyber security must simultaneously tackle both the social and technical realms, and that a rights based approach provides the proper framework for unifying both realms.

The study will demonstrate that a general system of property rights will provide a practical, robust solution for protecting the nation's critical cyber security infrastructure. The researchers recognize that a dialogue between developers of rights-based systems and cyberspace policymakers is needed to ensure that these technologies meet the broader needs of securing critical infrastructure, and that policies are aligned with the capability of new technologies.

Newly Funded Activities, Continued

Oral History on CIP Policy
Led by Roy Rosenzweig and Kathi Brown, Historian and Author

During the second year of funding, the CIP Project is going to sponsor the compilation and production of an oral history on critical infrastructure protection policy to be used in the public domain. The oral history will be compiled in three phases. The first phase of research will cover the period from the early 90's (in which a report was released by the Defense Science Board stressing the need to create a presidential commission to explore threats and vulnerabilities of critical infrastructures) to the actual establishment of the President's Commission on Critical Infrastructure Protection (PCCIP) in 1996 until the release of Critical Foundations (the Commissions report) and subsequently, Presidential Decision Directive 63 (PDD 63). The second and third phases will divide the period from the implementation of PDD 63 through the establishment of the Office of Homeland Security (OHS), then from OHS to the current day.

The data collection for this project will be done primarily through face-to-face interviews with participants, both panel members and Commissioners, of the PCCIP. The purpose of compiling such a historically relevant document is so that it can serve public and private actors working in CIP as a tool for lessons learned and best practices. Additionally, in the spirit of academia, the oral history will serve to advance knowledge and understanding in this arena.

This research will be conducted by three researchers. The principle investigator will be Dr. Roy Rosenzweig, GMU Distinguished Professor of History, and director of the Center for History and New Media. Prof. Rosenzweig has refined the oral history methodology through the use of digital archiving and interviewing. A GMU alum, and professional oral historian, Kathi Brown will be providing substantial direction, shape and leadership to the project. Ms. Brown recently completed an oral history for the cable industry called, "Wired to Win: Entrepreneurs of the American Cable Industry" and also penned the autobiography of J.W. "Bill" Marriott. Both CIP Project staff and School of Public Policy student, Rebecca Luria, will be conducting the majority of interviews and compiling the data. Finally, John McCarthy, Executive Director of the CIP Project, and formerly of the Critical Infrastructure Assurance Office (CIAO), will also be supporting this project.

Estimating Premiums for Insurance for the Health Insurance Portability and Accountability Act
Farrokh Alemi, Ph.D., GMU-College of Nursing and Health Science

Currently, insurance for HIPAA does not exist and this project proposes setting premiums for HIPAA insurance. This type of insurance is crucial to creating instant incentives for improving the security of health databases and operations. Insurance products transfer future risks into current premiums and an appropriate insurance product could levy higher premiums upon organizations taking excessive risk. In this sense, the insurance products create market incentives to secure health databases and operations. As information technologies change rapidly, creating a market incentive for more secure operations may be preferable to mandating security of data and operations through legislation.

The key deliverable of this research project will be the creation of a methodology for setting insurance premiums for HIPAA compliance. It will entail reviewing legislation and surveying hospital risk management groups to identify their current anticipated outlays under the HIPAA legislation. In order to estimate the yearly insurance premium, two pieces of information will be utilized: the potential financial outlays and the risks associated with the potential outlays. The College of Nursing and Health Science has extensive

(Continued, Page 8)

Newly Funded Activities, Continued

Alemi *(Cont. from Page 7)*
experience in conducting cost and risk analysis and would use the lessons learned in previous studies of expected costs to design this new methodology for assessing premiums for HIPAA insurance.

Current HIPAA legislation defines the potential penalties associated with accidental release of information. Additional financial outlays need to be estimated in the event of negligence that may result in a terrorist attack. A number of settled lawsuits establish the current financial outlays in cases of breach of privacy. The estimation of risk of a security breach and the quantification of this risk is more difficult than measuring the potential financial outlays. Since lack of experience precludes relying on existing data, this project will estimate the risks based on current multi-dimensional assessment methods. Organizations working on HIPAA compliance do not use a standardized approach to risk assessment, nor produce a single numerical measure of risk, thus the proposed research suggests constructing a numerical index of risk. The research proposes utilizing a panel of experts to make judgments regarding risk in health care institutions.

The Effect of the Tax System on Discouraging Investment in Critical Infrastructure
Led by Terrence Chorvat, GMU-School of Law

The current tax system discourages investment in risky ventures because of the asymmetrical way in which gains and losses are treated. For example, the investment of $20 million dollars in a venture that could make $20 million or lose $20 million (pre-tax) turns into one that could earn $13 million or lose more than $15 million. This asymmetrical treatment discourages investment in risky activities, and presents a problem for a number of tax payers. Insurance companies, which base their business on the assumption of risk, are taxed in the income they make. But, if the claims paid from a catastrophic event are larger than the income for a given year, the tax benefit of the deductions are less valuable than the tax cost of earning income. Insurance companies then charge higher rates, and are less likely to insure for high-risk events.

This problem of the tax system discouraging risk-taking can have a number of effects on the provision of critical infrastructure. First of all, critical infrastructure providers are likely to have their insurance premiums increased, because the effective cost of insurance is increased. Second, this asymmetry is likely to affect corporations that are not likely to turn a profit in the near future. Research initiatives that could be useful (but are not currently profitable) to critical infrastructures are put on the back-burner, because companies are not able to currently use the tax deductions or credits which accompany this research. Start-up enterprises cannot use their R&D credits and deductions at all, as they have yet to make a profit. Thus, useful activities are lost because of the tax asymmetry.

This research will examine three possible methods of addressing this problem. First, losses could result in refundable credits, which would create a benefit to match the detriment from earning income. Second, the tax system could allow interest to be paid on certain types of losses, allowing tax benefits to have the same present value as the cost of earning income. Finally, the tax system could allow taxpayers who are in a loss situation to sell their losses to profitable tax payers. This solution was proposed in the early 1980s, but was politically unpopular. This research will evaluate these three alternatives, and attempt to develop others.

Newly Funded Activities, Continued

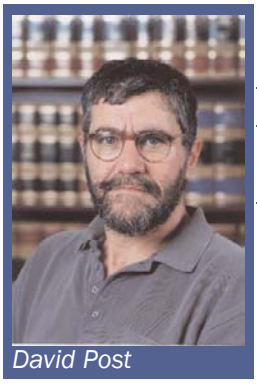
Regulatory Theory and Critical Infrastructure Protection
Led by Michael Abramowicz, GMU-School of Law

Professor Michael Abramowicz proposes to use the Defense Department's FutureMAP program to show how information markets can be used to support efficient regulatory decision-making. Although administrative law scholars have long considered a variety of tools to improve the quality of governmental decision-making, they have not considered this tool. Professor Abramowicz offers institutional and public choice explanations of how information markets can improve governmental decision-making.

FutureMAP seeks to test whether information markets can be used to make predictions about homeland security issues, such as the probability that terrorists will successfully disable parts of the nation's critical infrastructure. This kind of input could be valuable to regulators. As long as concerns about external manipulation of information markets can be neutralized, information markets can help agencies with objective predictions. This would effectively limit the twin dangers of agency capture and undue political influence.

The paper will also assess technical issues associated with information markets, suggest innovations to adapt information markets to a legal context, and describe possible applications for homeland security and more traditional regulatory contexts. Information markets might be used most effectively in conjunction with cost-benefit analysis, for example to make predictions about what the costs and benefits of various homeland security investments might be. Because the resulting predictions would be less manipulable and more flexible than traditional cost-benefit assessments, they would have a better chance of withstanding judicial review.

Critical Distributed Technology
Led by David Post and Richard Anders



David Post

One of the unique features of the technology landscape is the fact that certain technologies create "Standards Cages." A Standards Cage is a metaphor for all the goods and services that critically rely on a specific technology or standard. While the best known Standards Cage is the one formed by the Windows operating system, which contains virtually the entire PC software industry, there are many other such Standards Cages within our economy.

There has been a significant amount of work on the economics of Standards Cages, and on their implications for competitive activity. Much less attention - perhaps none - has been directed at a series of questions that should attain more prominence as the result of the events of September 11, 2001, namely: how do the inbred ecosystems of Standards Cages impact national security and economic growth, and what, if anything, might we do to begin to address these vulnerabilities?

The paper will examine the steps that can, and should, be taken to ensure that industries within Standards Cages are secure and promote efficiency. Many of the underlying technologies that create Standards Cages are, themselves, the product of protective legal regimes, involving patent, copyright, trademark, and related laws; this paper will look at the extent to which these (or other) legal regimes can or should be enlisted to minimize potential security vulnerabilities.

Newly Funded Activities, Continued

Mitigation of Terrorist Inspired Events
Led by Roger R. Stough, GMU-School of Public Policy

This research program will expand the Stargazer- NET platform and its disaster mitigation communication system through collaboration with the Stargazer Foundation. Operating as a non-profit public charity, the Stargazer Foundation has developed a global Internet platform - StargazerNET, which is strategically partnered with the George Mason University. Providing free services such as distance learning tools, message boards, E-surveys, and chatrooms, StargazerNET has also created a unique disaster mitigation system known as ReadyLink that enables, people, groups, and organizations to stay in touch with each other and to access critical news and health and safety information during and after an emergency. To this end, it is expected that ReadyLink will become an integral part of the Homeland Security Preparedness strategy and plan across America over the near term future.

The objective of the research program being undertaken through the CIP Project is to meet the anticipated demand for ReadyLink and to improve the security modules and disaster recovery strategies to make the service more impervious to both physical and virtual attack. In addition, the program will support the dissemination of information about the availability of the tools that support ReadyLink, as well as the need for a training program in the use of the tools. The program proposes an extensive research effort that will result in journal articles focused on the theoretical, technical, and policy issues regarding disaster mitigation.

Protection of the Post in the Early Republic
Led by Ross Davies, GMU-School of Law

Although Presidential Decision Directive 63 identified and defined "critical infrastructure protection," in the 1990s, it was not a new concept for the United States. Throughout American history, the country has relied on various systems to sustain daily life: the highway system in the 1960s; the rail system during the Industrial Revolution; and the postal system in the days of the early republic. The legal history surrounding the old postal system can provide important lessons about the development of modern critical infrastructure protection.

The early postal service was - as every leading figure of the era who addressed the subject acknowledged - a uniquely critical piece of the early national infrastructure. As the Post Office's original organic act announced, "the communication of intelligence with regularity and dispatch from one part to another of the United States is essentially requisite to the safety as well as the commercial interest thereof." Establishing the integrity of the mail system was a serious concern to the early government. Much like our current critical infrastructures, the success of the mail system depended on public-private relationships. For example, during the War of 1812, government postal service to New Orleans was cut-off, but private entrepreneurs stepped in to fill the gaps. Eventually, competition among contractors provided market forces to improve this important public service.

This paper will focus on the legal and operational approaches to securing the post roads and post offices, and on the way those approaches were treated in the three branches of government. The Post Office's unique position as both a critical publicly owned component of the nation's commercial-governmental-military-social infrastructure and an organization subject to powerful private forces, make its history a promising source of experience and precedent for today's critical infrastructure protection scholarship.

Newly Funded Activities, Continued

Cybersecurity in Financial Markets: An Investigation of Network Regulation
Led by D. Bruce Johnsen and Supriya Sarnikar, GMU-School of Law


Johnsen

Our national economy depends on a secure financial system. Much of our industrial, technological, agricultural, and even national defense activity relies heavily on investment capital raised within, or intermediated through, the U.S. financial system. What is more, the prices generated by our various financial trading systems serve as invaluable signals for efficient investment and resource allocation decisions by countless operating entities. The interdependencies generated between the various financial institutions make them especially attractive targets for terrorist attack: if one part goes down, the whole system is affected.

Yet, U.S. financial market regulations over the past 30 years have actually increased the vulnerability of our trading systems to cyber terrorism by mandating a "national market system" in which otherwise separate trading systems are electronically linked into a single integrated network. Through these regulations Congress and the U.S. Securities and Exchange Commission (SEC) have arguably achieved their goal of improved price uniformity and transparency. But price uniformity and transparency are not ends in themselves. The degree to which they benefit the national economy depends on their costs, and the recent increase in the threat of cyber terrorism has decidedly increased these costs, presumably reducing the optimal extent of network integration as a result.

The question this research addresses is whether, to what extent, and under what circumstances it is in the national interest to maintain the national market system in light of the increased threat of network-directed cyber terrorism. There are two possibilities: one, that the SEC actively police the cybersecurity investments made by network participants, and mandate additional investments when they fall short; or a more plausible alternative is to restore the various participants' proprietary stake in their own trading systems. This project will involve a thorough review of the electronic linkages mandated by the SEC, careful identification of the associated network effects, an in-depth analysis of any maligned incentives for cybersecurity the mandated linkages might create, and a practical assessment of possible solutions.

The Economic Regulation Of Transportation And Of Cyber Space
Led by Kenneth Button, GMU-School of Public Policy

The aim of this project is to examine the developments that have taken place in the thinking about the regulation of a network sector such as transportation, and to contrast this with the requirements for regulation of cyber space. The network characteristic of both transportation and cyber space provides a fundamental link between them. They also have diversity in common and both involve the supply of an intermediate product (with associated issues of derived demand). Although transportation is clearly a more mature sector than cyber space, it is dynamic and much attention has been centered on regulatory regimes that minimize distortions from overbroad regulation. Because transportation has been the subject of a diverse range of economic regulations and has undergone a significant process of regulatory reform, it provides a rich resource for assessing how emerging sectors with similar features may be efficiently regulated.

The study would be limited to looking at relevance of the economic regulation ('quantity regulation' to adopt the European jargon) of transportation to cyber space, and not at social

(Continued, Page 12)

Newly Funded Activities, Continued

Button *(Cont. from Page 11)*
regulation of such things as environmental intrusion. The emphasis will therefore be on matters such as efficient market structure, innovation and consumer protection in the most general forms. It will look at the foundation of various approaches and instruments and will cover the entire gamut of relevant regulatory approaches ranging from theories of public ownership at one extreme, to those of moral suasion at the other. Equally, instruments will embrace command-and-control instruments, ranging through pricing and taxation to self-regulation.

The analysis will be largely at a conceptual and theoretical level focused primarily on the intellectual underpinnings of regulation. Resulting in a report as well as articles, the findings will be assessed in terms of not only the usefulness of the various models of regulation to transportation, but also their potential as tools for regulation of cyber space.

Economic Analysis of Cybersecurity
Led by Bruce Kobayashi, GMU-School of Law

The study of law and economics teaches us to look not at what is "fair" on its face, but rather what is most cost-effective. Weighing the costs and benefits of a certain plan or outcome, which is better? How are resources best used? What is the most efficient outcome? These concerns also need to be taken into account for cybersecurity: should it be security at any cost, or can efficiencies be built in that makes it more cost-effective to participate? What are the incentives to be secure?

This research will provide an economic analysis of the positive incentives for the provision of minimum-security standards on computer networks, and of the provision of sanctions for non-compliance with such minimum standards. The paper will analyze the positive and negative spillovers associated with the provision of security on computer networks, and will use as a basic framework the existing law and economics literature on the private enforcement of law. It will also analyze why ex-ante prevention through the use of minimum security standards is likely to be preferred to ex-post sanctions.

The paper will then examine various ways in which positive incentives for private firms or groups of firms to provide security on computer networks can be created. The recent literature on intellectual property rights and standard setting organizations imposes bylaw and contract restrictions on members, business method patents, provisions of the copyright laws (including the DMCA's anti circumvention provisions), trademark laws, and trade secret laws. The paper will consider the appropriate scope of any such protection, including the issue of whether the "owner" of a cyber security standard should be able to appropriate the gains from the benefits of the network that are not related to the superiority of the particular invention. Finally, the paper will examine the sanctions/enforcement side, including use of expulsion in conjunction with the use of reputational and other bonding devices. The paper will also examine the adequacy and availability of contract and intellectual property damages.

Newly Funded Activities, Continued

Proactive Infrastructure Security: Evolutionary Generation of Terrorism Scenarios
Stage I: Feasibility Study and Building Demonstration Systems
Led by Tomasz Arciszewski, GMU-Civil, Environmental and Infrastructure Engineering

Providing infrastructure security is extremely difficult when dealing with an enemy that is using asymmetric measures--that is to say an approach that is directed against a nation's vulnerabilities and weaknesses, while ignoring its strengths. Countering this approach requires a great deal of strategic thinking and restructuring to successfully undertake fourth-generation warfare against asymmetric threats - the kind of threats generally posed by terrorist networks. A proactive approach to security in the face of asymmetric threats calls for the generation of a wide range of terrorism scenarios, the selection of an appropriate scenario to best correspond to an evolving actual situation, and the preparation of appropriate countermeasures. The purpose of this study is to initiate development of an entire technology for proactive infrastructure security through the generation of the most dangerous terrorism scenarios.

The strategic research objective of this project is to develop a process, an associated set of methods, and computer tools for the generation of terrorism scenarios that will be based on the principles of information technology and knowledge management. The researchers also suggest creation of an activity group that would produce, modify and maintain a large suite of integrated processes and tools for terrorism scenario generation, which could be used by federal, state, and local agencies, either deployed or as a centralized resource. The tactical (short term/Stage I) research objective is to develop two demonstration systems for two different audiences.

The first demonstration system is intended to demonstrate the nature and feasibility of computer tools for generating terrorism scenarios. Its audience will be selected focus groups, emergency management officials, National Guard leadership, and homeland security officials. It will be prepared for the generation of terrorism scenarios describing potential terrorist attacks on the central part of Washington DC. The system will be based on evolutionary computation and will be developed using Inventor 2003. The second demonstration system is intended for water supply professionals. The first component of the system will be the experimental tool TerrorMax/Herndon developed in the IT&E School for the generation of terrorist scenarios for the water supply system in the City of Herndon. The system is complex and its use requires expertise and time. Therefore, the second component of a proposed demo will be a presentation providing a description of TerrorMax/ Herndon and an overview of various results produced by the system.

Bletchley Park, Enigma, and Information-Sharing Solutions
Led by Peter Harter, GMU-School of Law

Today, information sharing is developing as a regular practice in the private sector through ad hoc relationships between individuals, professional associations, contractual obligations, and public-private partnerships. Collaboration between countries, companies, industry sectors, etc. occurs more out of necessity than regulatory mandate. Over 65 years ago at Bletchley Park in the UK, innovations in business processes, professional relations, and technology occurred, despite heavy military and governmental involvement. Such innovations resulted in part from the nature of how information was gathered and processed, integrated with other sources, and then shared.
(Continued, Page 14)

Newly Funded Activities, Continued

Harter *(Cont. from Page 13)*
Technology and massive amounts of data necessitated this; but from this necessity Colossus, one of the first computers, was born. And the Nazi secrecy code, Enigma, was broken.

Many useful lessons can be learned from the rich history of Bletchley Park and how it broke the Enigma code. Solutions for international information sharing practices can be discovered, as well as the human resources that made such information sharing possible. The barriers to information sharing that existed during World War II still exist today, and this research will help public and private policy makers appreciate and overcome such barriers when working towards a common goal. It will also prepare leaders for the debates and hard decisions they have to make on how and why to share information and collaborate.

This research will examine the practices at Bletchley Park and extract those lessons that are useful to the current world of critical infrastructure protection. It will compare past and current legal systems, and the role of the private sector then and now. The lessons learned at Bletchley park can be projected into agreements and practices used by multinational corporations that struggle with the dilemma of gathering and sharing information across borders.

Transportation Infrastructure Security: Innovative Technology for Vehicle, Operator and Cargo Identification Led by Professor Michael Bronzini, GMU-Civil, Environmental, and Infrastructure Engineering

Obtaining data on processes and subjects of interest is a critical part of homeland security. This data requirement extends to information about vehicular traffic in the transportation system. Traditional traffic sensing and surveillance systems focus on macroscopic stream measures, such as traffic volume, speed, and density, and vehicle classification (passenger cars, buses, trucks). In some cases individual vehicle speeds and space-time trajectories are observed. In the new era of security concerns it is often imperative to identify specific vehicles and operators, and the cargo in the vehicles.

The ultimate objective of the Transportation Infrastructure Security study is to create a transportation data collection system with the ability to identify vehicles, operators, and contents. This will require use of both traditional and innovative vehicle detection technologies, and advanced data fusion systems to marry real-time vehicle observations with motor vehicle record systems and other relevant information systems. New technologies to be investigated include remote sensing, hyperspectral imaging, real-time image processing, data mining, and data fusion.

George Mason already has extensive experience and expertise in all of the relevant technologies, including international leadership in applications of remote sensing and hyperspectral imaging to transportation flow measurement. This initial project will focus on developing detailed system requirements and identifying promising system concepts and technological elements. Another product will be a presentation package that demonstrates the importance and benefits of this type of system. Consideration of institutional, societal, and legal issues will occur throughout the project.

Newly Funded Activities, Continued

Racial Profiling: The Conservative Case Against Racial Profiling in the War on Terrorism
Led by Nelson Lund, GMU-School of Law

Since 9/11, public opinion polls have shown strong majorities in favor of subjecting those of Arab descent to extra scrutiny at airports. By now, the sight of little old ladies stopped for humiliating random searches at the boarding gates is quite familiar - while far more dangerous looking men have walked down the jetways without so much as a second look from the security screeners. Political correctness, obsessive pandering to racial sensitivities, bureaucratic mindlessness - whatever the diagnoses, the cure is taken to be obvious: get serious about protecting us from another attack, which we can be quite sure will not be carried out by septuagenarian Norwegian-American women.

But the new enthusiasm for racial profiling is misguided, for three reasons. First, racial profiling or stereotyping is something that we do all the time; although there are good reasons to do it, there are reasons why we shouldn't do too much of it. Second, free societies and markets foster profound sources that tend to curb irrational racial stereotyping. Third, governments are highly prone to excessive racial stereotyping and are largely immune from the forces that keep this practice in check in the private sector; thus, government policies that engender racial profiling should be treated with skepticism.

This research will explore these themes in greater depth, cultivating the conservative argument against racial profiling. Although conservatives traditionally support aggressive law enforcement techniques (and are less likely to believe that police officers are prone to racist behavior), the conservative views against profiling are compelling. Most of all, racial profiling undermines the important national goal of making all races equal under the law.

Building Undergraduate Security Curriculum
Led by Anne Marchant, GMU-IT Undergraduate Education
Edgar H Sibley, GMU-Information and Software Engineering and Public Policy
Hugh Tazewell (Taz) Daughtrey Jr., JMU-Institute for Infrastructure and Information Assurance

Sibley

Even prior to the shocking and tragic events of September 11, 2001, it was evident to many that our nation's information security infrastructure needed strengthening. Web hacking incidents and the proliferation of rogue programs have served as warnings that our society's increasing dependence on the Internet has created an exposed flank. Developing well-dispersed undergraduate programs in security can be one strategy to help improve our nation's overall information security defense.

This project proposes the development of cyber-defense curricula for the State of Virginia and the USA as a whole, beginning with George Mason University and James Madison University students. Specifically, the intent is to develop the curriculum for undergraduate students at both institutions and insert it into the current streams in the Summer and Fall semesters of 2004. A pilot program will be employed during the Fall 2003 and Spring 2004 with doctoral and masters candidates.

The undergraduate security curriculum will include coursework in programming, operating systems, and networking, as a basis for the major courses in security. Modules in ethics and social

(Continued, Page 16)

Newly Funded Activities, Continued


Daughtrey

Marchant *(Cont. from Page 15)* responsibility must also be woven into this coursework. A capstone course including cyber-defense exercises, such as those performed at West Point have proven effective. The goal is to develop a set of courses that will afford capable students an opportunity to become a security engineer. Furthermore, the final exercise will serve as an assessment tool that will measure the success of course outcomes and proves their value in real life situations. Top undergraduate and graduate students from both the George Mason University and the James Madison University will be chosen to participate in the Cyber-defense exercises Technical expertise will be drawn from networking and high-confidence laboratories currently being expanded in the Commonwealth Information Security Center at JMU.

By combining the resources of faculty and students at two state institutions in this joint project, benefits can be maximized. Not only will the duplication of effort be avoided, but also cross-pollinating ideas that will lead to more successful teaching strategies.

Using Unfair Competition Liability to Backstop Industry Self-Regulation
Led by Jane Kaufman Winn, GMU-School of Law

In the absence of any general US legal requirements governing the use of personal information, the Federal Trade Commission has used a combination of voluntary disclosure of privacy policies combined with unfair trade practices enforcement action to increase the level of data protection offered to citizens. In the realm of policy-based computer security standards, unfair competition and deceptive trade practices laws may be able to provide a private cause of action that would increase the level of computer security standards compliance in commerce. This study reviews the provisions of the Uniform Deceptive Trade Practices Act and federal trade law such as Section 43(a) of the Lanham Act to determine whether private rights of action under those laws could provide effective solutions for industry self-regulation efforts aimed at increasing critical infrastructure protection.

The Bush administration has made a concerted effort to promote self-regulation for cybersecurity, instead of imposing new government regulations. In the information privacy arena, several innovative self-regulation strategies are now being tested. The technology and policy issues encountered in securing networked systems and in guaranteeing information privacy rights are often very similar; thus, privacy law innovations may be useful models for developing computer security self-regulation. For example, the US-EU Data Protection Safe Harbor agreement encourages self-regulation by setting out data protection standards that US organizations must meet in order to receive personal data from EU sources.

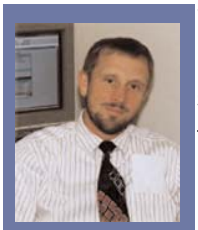
This type of standards-setting will play an essential role in raising the level of computer security throughout networks, while assuring interoperability. Some standards will be technical, and compliance with these can be established through review and certification from independent third parties. Other standards will address business practices and organization policies, and must be implemented by the staff of an organization. These policy standards should contain mandatory independent audit and certification elements, to avoid problems if companies claim they are in compliance when they are not.

Newly Funded Activities, Continued

A Decision Support System for Hazardous Materials Accidents and Terrorism Response

Michael L Deaton, PhD[1]; Mark A Kirk, MD[2]; Stephen Frysinger, PhD[1]

[1]College of Integrated Science and Technology, James Madison University, [2]Division of Medical Toxicology, Department of Emergency Medicine, University of Virginia



Deaton

Kirk

Frysinger

We are creating a prototype decision support system (DSS) for local and regional preparedness planning and emergency response. This system will integrate robust federal, state and local chemical inventory databases (such as SARA TITLE III, HSEES, and TRI), medical response data, and medical readiness data into an easy to use tool. The DSS will use process models, population data, and risk assessment tools with a comprehensive Geographic Information System (GIS).

The project objective is to develop a standardized, but easily adaptable vulnerability assessment tool that will enable planners at the local, regional, state, and national levels to identify those chemically-related events for which communities are most vulnerable and least prepared. Such a tool will provide a powerful platform for planners to utilize federally mandated data to guide planning efforts, thereby making the most efficient use of resources.

Moreover, this system will help create a bridge between federal resources and local emergency preparedness. This bridge will help some federal agencies, such as the Agency for Toxic Substance and Disease Registry to integrate its data with local resources at a local level and to identify local data resources that would enhance the federal databases. The decision support system will serve as a strategic planning tool for poison centers and medical toxicologists to integrate their services and expertise about chemical emergencies into local and regional response plans. With this tool, medical toxicologists can identify training needs and create courses to teach firefighters, EMS personnel, nurses, and physicians about their community's greatest risks regarding chemical emergencies.

A fully functional working prototype is expected by May 2004.

Constitutional Pliability Rules

Led by Eugene Kontorovich, GMU-School of Law

In the wake of a massive terrorist attack, the government makes large-scale arrests in an attempt to prevent new attacks. Detainees are not swept in on the basis of individualized suspicion, but the goal is not to arrest people guilty of a crime. Such mass detentions are necessarily overbroad: they sweep in many innocent people with those few that are planning terror attacks. Under current standards, if a detainee brings suit for his freedom, a judge only has two choices: either issue an injunction whereby all detainees are released; or find that the danger to society outweighs the individual interests in liberty, and uphold the detention. But is there a middle ground, where both the rights of the individual and the interests of the state can be upheld: "constitutional pliability rules."

The individual liberties set out in the Bill of Rights are commonly thought of as property rights, to be protected by property rules. This means that the government can take these rights only with the agreement of the citizen. If these rights are violated, the remedy is an injunction. But under "pliability rules," another

(Continued, Page 18)

Newly Funded Activities, Continued

Kontorovich *(Cont. from Page 17)*
option becomes available: upon the finding that emergency measures such as mass detentions invade individual rights, the court can refuse injunction but award tort damages. The detainees would be compensated for the invasion of their rights. The constitutional pliability system could have property rules as the default remedy, but upon the happening of certain contingencies (i.e. national security concerns) the protection would temporarily toggle to a liability rule for the duration of the contingencies.

Constitutional pliability rules will make courts much better equipped to deal with large scale law enforcement responses to terrorism. By allowing compensation for detainees, the pliability rule regime will increase the chances that courts will not nix mass detentions when they are needed, while providing protections for individuals they do not currently enjoy.

Supervisory Control And Data Acquisition (SCADA) Systems Security Critical to our Manufacturing Infrastructure

Led by Dr. Geoffrey Egekwu, JMU-Integrated Science & Technology Program

The services provided by a supervisory and data acquisition (SCADA) system for a manufacturing enterprise includes messaging, diagnosis, alarms/events, history of activities, visualization, and device integration. These services constitute critical national infrastructure that must be protected from intrusion and corruption.

A typical SCADA system monitors and controls a number of critical plant floor sub-systems - the so-called islands of automation. The SCADA therefore manages very complex and inter-related data and information networks including: computer-integrated manufacturing (CIM) systems, intelligent warehouse systems, computer-aided manufacturing (CAD) systems, computer-aided engineering (CAE) systems, and operations management systems. The security challenge of the SCADA system is compounded by the fact that the relevant data and information networks must now be connected to external public and/or private networks (customers, suppliers, collaborators, government agencies, consultants, etc.). The potential entry points by an intruder increase exponentially - therefore a single breach anywhere in the network can affect the operations of multiple manufacturing enterprises.

We are studying methods that can enable an enterprise to prevent intrusion from happening in the first place by employing multiple security solutions within an integrated system. The possibility of a hardware-based security system, which will translate to the deployment of multiple sensors at critical node points in a SCADA network, are being evaluated in this study.

We are currently configuring new factory suite software in the Engineering & Manufacturing laboratory of Integrated Science & Technology program at James Madison University with full control (SCADA) and coordination (supplier and customer supply chain links) capabilities - generally referred to as a manufacturing execution system. The software can also provide real-time linkages to other internal and external networks. We plan to use this software to aid in isolating critical points in a SCADA network and study methods of protecting them.

Because threats for an information system come from both outside and inside sources, a holistic protection strategy is needed to provide embedded and redundant security layers that protect information assets - FBI studies have shown that 80% of intrusions and attacks come from within organizations. We have designed such a system that will soon be tested at our manufacturing laboratory. This integrated full-scale network solution combines the latest technology in digital surveillance, access control, physical asset management, building management, alarm monitoring and control with biometrics on a single hardware and software platform. The tools will enable us to overlay an enterprise risk management lifecycle model over our security system.

Newly Funded Activities, Continued

Time Domain Probabilistic Risk Assessment Tool Development At James Madison University

Dr. George H. Baker, JMU-Integrated Science and Technology

An important technique for assessing the types of possible failures and their respective likelihoods is probabilistic risk assessment (PRA). To analyze and quantify survivability, conventional probabilistic risk assessment methods provide a snapshot of potential failure modes at a single point in time for certain initiating conditions. James Madison University is perfecting a new technique that improves upon existing PRA by adding the time dimension to the evaluation of failure modes of interdependent systems.

The technique is being prototyped using the LabView graphical programming language. LabView allows the development of visually appealing and intuitive user interfaces. These interfaces can be developed with minimal programming experience. For probabilistic modeling, each system component is described by a separate subroutine. Individual component status indicators can be displayed and changed according to the scenario of interest.

Once developed, these individual component subroutines can be easily connected or "wired" together through logic icons. As an initial test case, we are using a hypothetical communications center.

Based on the system functional diagram, a fault tree is derived that contains the Boolean relationships among the system elements. The element states are green or red depending upon whether the element is functioning or not. The initial states of the components are programmed based on the scenarios of interest. The fault tree determines how effects on single or combinations of system elements propagate and ultimately indicates whether the total system can perform its mission. The code is being developed to compute system reconstitution times based on repair times for individual elements and repair sequences (e.g. in many cases it is necessary to reconstitute electric power before other systems can be serviced).

The code advances the clock in discrete time steps. Using a basic Monte Carlo simulation the code will produce a graph of Po(t), the probability that the system is out of service up to time *t* based on the specified scenario.

By convolving the code output with outage cost values, C(t), one can estimate the probable value of lost services.

The code is oriented to simple, top-level risk assessments of physical infrastructure systems. We have demonstrated proof-of-principal for the time domain risk assessment technique and are now testing its usefulness and validity for real system problems. We note that successful code application requires that it be used as part of a well-defined risk assessment methodology and that system experts be involved in defining input parameters to ensure reliable results.

Law, Economics, and - Outreach

It's been a year of great conferences here at the CIP Project.

by Emily Frye

As Stewart Baker, one of the leading lights in cyberlaw, said to me once, "You have to do the work, and you have to find time to talk about the work." One of the biggest challenges for Critical Infrastructure Protection is that most people don't know about it. Those who do know about it rarely circulate outside their own circles, so getting the word out to a broader community is vital to increasing the level of knowledge and effort that goes toward protecting our critical infrastructures.

October 2002 saw the first Tech Center conference on cybercrime, which brought together leaders in government, industry, and academia to discuss important policy issues related to the technological methods, international cooperation challenges, and public sector-private sector aspects of cybercrime.

In January 2003, the CIP Project kicked off its own series of unique conferences. Each was designed to address an important but poorly understood area of critical infrastructure, as well as to bring together constituencies that would not normally be drawn into a common discussion.

First came "Information Sharing and Antitrust: Identifying Issues, Creating Solutions," on January 30. Industry leaders and government officials convened to discuss whether antitrust can be seen as a meaningful impediment to information-sharing that is designed to improve critical infrastructure protection. Since so much of critical infrastructure is owned and operated by the private sector, but national defense resides in the public sector, there is clearly a need for widespread information sharing to protect these entwined areas of responsibility. Dean Mark Grady raised the importance of non-traditional solutions to non-traditional problems, such as relying on private industry to generate answers before looking to regulation. 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. John Tritak, the first Executive Director of the Critical Infrastructure Assurance Office, forced the attendees to confront the costs of not sharing information. By stressing that antitrust issues are not necessarily an impediment to ISACs, the speakers opened the door to facing a heretofore unacknowledged truth: it's fear that really stops information sharing - fear of liability and fear of competitive disadvantage.

On March 28, "Open-Source Software, Proprietary Software: Implications for National and Economic Security" lured nearly one hundred intrigued industry participants and policymakers to the School of Law. One participant remarked that it was a group that had never before been assembled, crossing the boundaries of the traditional interest groups, which have grown more entrenched over time. A range of speakers presented the arguments and reasoning behind their approaches to software development. Representatives from large proprietary software companies, such as Microsoft and Wind River Systems, presented their views; and the author of the MITRE report about Department of Defense use of free and open-source software also spoke. Free and open-source software programs have already become part of many networked systems - including national defense systems - and the clock isn't turning backwards. What we learned at this conference is helping build a report on open-source software that the CIP Project will publish within the year.

"Legal Questions at the Forefront of National Security" brought together a diverse group of practicing lawyers, policy professors, and academics on May 9 for a day of pondering the big questions facing the CIP community. With people like David Rivkin and Tim Edgar as discussants, we asked "what is the proper forum for prosecuting terrorists?" Looking to leaders like former Chief Counsel for Privacy at the Office Management and Budget Peter Swire, we attempted to generate a guideline for socially optimal amounts of self-help in the

(Continued, Page 23)

In preparation for the first event of the "CIP Project Critical Conversations" series, which was held on June 18th, U.S. Representative Christopher Cox (R-Cal), Chairman, Homeland Security Select Committee, shared some of his thoughts with Frank Sesno, Senior Fellow to the CIP Project.

Sesno: Let's start by addressing the issue of priorities. As you look at critical infrastructure, where should we be paying most attention now?

Cox: Well, of course when I look at priorities, because I am coming at this as Chairman of the oversight committee for the Department of Homeland Security, I look more often at the Department's priorities, and if I may answer the question from that perspective, our overarching focus - which includes infrastructure protection - is to develop its statutorily mandated intelligence analysis capability.

With respect to infrastructure protection, [developing intelligence analysis capability] is vital because threat-based analysis of both vulnerabilities and responses is ultimately all that we are capable of achieving. If it's not a threat-based analysis, if it's simply an analysis of our vulnerabilities, then we'll run out of GDP to pay for all of the hardening that needs to take place. Indeed that may be the challenge anyway because the best intelligence may lead you inexorably to the notion that terrorists are going to constantly bob and weave and look for the soft underbelly of whatever you have hardened yet that is what they are going to hit.

But most important of all, is to recognize what the Administration and Congress had in mind in writing the legislation by creating intelligence analytical capability within the Department. If Secretary Ridge cannot place requirements on the intelligence

Congressman Chris Cox

community and if the community is not providing him or the Department a lot of analyzed information that they can sift through from their vantage point and through their lens, then they won't be able to make the decisions that need to be made. Thus they won't be able to give us an accurate list of what our vulnerabilities are, they won't be able to tell us, "Here are the priorities." This is really a prerequisite to any priority analysis.

Sesno: Based on the threat assessment that we have, where would you say the priorities would be in protecting critical infrastructure?

Cox: There's only one category in IP [infrastructure protection] that you could even remotely see in advance. Items in this category are so critical that if they were destroyed, the economy's ability to function, the nation's ability to function would be seriously compromised. This category is comprised of a very small number of items.

Sesno: What about cyber protection?

Cox: Well, cyber as a means of [allowing us to] accomplish [certain objectives]. [For example,] if you deprived the nation of information for an extended period of time, you would probably deprive it of power and communication in the process. That would be very consequential.

But chemical, for example, is in the second category, where the risk is massive loss of life.

You need to have an appreciation of what our enemies are thinking about, what they understand, what they know how to do. Not knowing what our enemies have and having to protect against everything quickly breaks the bank.

Sesno: With respect to critical infrastructure, obviously there is a great deal of discussion of the role of private sector. Can we incentivize infrastructure protection? Where exactly do you think we should be taking that as a matter of conversational policy? *(Continued, Page 22)*

Virginia Institute for Defense and Homeland Security

The Virginia Institute for Defense and Homeland Security (IDHS) is a university and industry research consortium, created in February of this year, which is dedicated to delivering solutions that support the United States' homeland security and defense objectives. The Virginia IDHS will conduct research, education, and technology transfer at member institutions and firms with an emphasis in the fields of telecommunications, biodefense, sensor systems, and risk management. Additionally, industry consortium members will commercialize technology and develop solutions that support rapid deployment.

The 2003 Research Summit, which was held on June 25th, established a forum for a variety of IDHS' university partners to present some of the innovative research they are conducting. The Summit provided an opportunity to facilitate collaboration among the participating universities in Virginia as well as inform other stakeholders about the exciting ongoing work. ❖

IDHS is working with a variety of university and industry partners, which include:

College of William and Mary
Eastern Virginia Medical School
George Mason University
George Washington University Virginia Campus
Hampton University
James Madison University
Norfolk State University
Old Dominion University
Shenandoah University
University of Virginia
Virginia Commonwealth University
Virginia Military Institute
Virginia Polytechnic Institute and State University
Virginia State University
Virginia's Center for Innovative Technology


Cable Risdon Photography

Frank Sesno

Cox *(Cont. from Page 21)*

Cox: I think we need to connect the potential liability that exists after the next terrorist attack with the government's ability to protect the private sector and consumers derivatively from that in exchange for responsible steps to protect critical infrastructure.

Sesno: *So is this legislative?*

Cox: This would have to be legislative, but an enabling feature of the legislation would be that the Department of Homeland Security could, through clear guidance and regulation, describe what responsible behaviors permit one to reside within a safe harbor.❖

Conferences *(Cont. from Page 20)* cybersphere. To round out a day of difficult questions, we sought the counsel of ethicists like Amitai Etzioni and free-press advocates like Lucy Dalglish in determining what limits should surround government efforts to control terrorism.

The CIP Project coordinated two more conferences in the month of June. Working with the Tech Center and the Progress and Freedom Foundation, we helped build "Promoting Markets in Creativity: Copyright in the Internet Age." One of the highlights was CIP Project friend Katherine Lawrence, author of Creativity at Work, who shed light on the practical aspects of human motivation into a discussion of legal incentive structures.

With support from the American Bankers Association, the CIP Project and the FDIC lined up an informative day of impressive speakers to bring the management of midsize banks up to speed on "Cyber Risk Management: A Comprehensive Look at Handling Cyber Risk."

After taking stock of the past year's learning opportunities, we are planning another year of stimulating intellectual offerings. Stay tuned for more news about upcoming conferences on "The Law and Economics of Cybersecurity" and "Emerging Regulation to Secure U.S. Ports." ❖

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 June 2002. The CIP Project encourages participation by representatives from all levels of government, academia, and private industry.

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

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