The CIP Report

VOLUME 1, ISSUE 1 JULY 2002

Welcome to the Inaugural Edition of *The CIP Report*

Each month, the CIP Project will publish an electronic newsletter focusing on Critical Infrastructure Protection. This is intended to be an educational newsletter that brings together current information for industry, government, and academic professionals with an interest in CIP. Although this first issue provides background information on critical infrastructure protection, each subsequent issue will focus on an individual sector, such as banking and finance, telecommunications, and transportation. The newsletter will highlight sector initiatives, Information Sharing and Analysis Centers (ISACs), industry leaders, and the most relevant issues. The newsletter will also provide the latest news in critical infrastructure protection, emerging legislation, government initiatives and leaders, and academic endeavors.

Please send any comments to cipp01@gmu.edu. Your thoughts are always welcome. We hope that you find *The CIP Report* an interesting and informative newsletter.

Message from Richard A. Clarke Special Advisor to the President for Cyberspace Security

I would like to formally welcome the CIP Project into the national critical infrastructure protection debate. The launch of the CIP Project coincides with this year's release of the National Strategy to Secure Cyberspace. The purpose of this strategy is to have a nationally accepted game plan to secure cyberspace at all levels--from government to industry and academia, to the single computer in a home office. The strategy will delineate vulnerabilities at five levels of society, the largest of which is national level institutions, such as banking, telecommunications, transportation, etc. I expect that the CIP Project will make significant contributions to this national strategy, particularly at this sector level. The combination of academic resources, along with the Project's dedication to examining critical issues in technology, policy, and law, will result in what I hope is a robust program at the cutting edge of critical infrastructure protection.

A Brief History of Critical Infrastructure Protection at the National Level

The development of the nation's energy, water, telecommunications, finance, water, and transportation systems, as well as the infrastructure on which government delivers critical services, brought both rapid advancements and increasing vulnerabilities to our nation. Efforts to protect these systems are as old as the systems themselves. But with the introduction of computer systems into the core operations of these basic infrastructures, protecting them became increasingly complicated.

In the aftermath of the tragic bombing in Oklahoma City, the Federal government commissioned a working group to study emerging threats and vulnerabilities, and the national

(continued, Page 5)

George Mason University School of Law's National Center for Technology & Law, in Conjunction with James Madison University, Launches Critical Infrastructure Protection Project

ARLINGTON, VA (May 14, 2002) -- Rep. Frank Wolf (R-Va), George Mason University President Alan Merten, James Madison University President Linwood Rose, and George Mason University School of Law's Dean Mark Grady today formally launched the Critical Infrastructure Protection Project (CIP Project), a collaborative effort led by George Mason University School of Law's National Center for Technology & Law, in conjunction with James Madison University.

The CIP Project is funded by a $6.5 million National Institute of Standards and Technology grant at the direction of the House Appropriations Subcommittee on Commerce, Justice, State and the Judiciary, which Congressman Wolf chairs.

"Congressman Wolf's leadership in the homeland security and critical infrastructure protection objectives is targeted at filling a serious gap in the nation's ability to prepare for, respond to, and recover from significant cyber-based infrastructure attacks," said John McCarthy, the CIP Project's Executive Director. McCarthy noted that senior leaders in business, government and academia are struggling with a variety of technological and non-technological impediments to managing cyber-related risks. Many of these impediments involve intricate questions of law, policy, and business processes and their relationship to technological applications. Some examples include tort liability, information sharing among competitors for security purposes, and exchange of information between business and government to improve cooperation for managing national security risks.

"Our intent is for the CIP Project to generate real solutions that address the complex legal, policy and technology issues associated with an increasing number of cyber attacks and cyber failures affecting government agencies, military, private sector businesses and even individuals," McCarthy said.

The CIP Project's four program elements include:

- Providing Education and Outreach -- seminars and workshops, professional education and training, and facilitated government-industry-academic industry discussions.
- Serving as a repository of expertise for government and industry -- Because cyber security issues are not generally well understood, there is a need for expertise in a range of issue areas. Government support includes developing model legislation covering cyber-security issues and testifying on complex issues of law, policy and technology.
- Sponsoring research -- While there is no single source of excellence in cyber security law and policy, both George Mason University and James Madison University are recognized by the National Security Agency as Centers of Excellence for Cyber Security. Leveraging the universities' expertise, the CIP Project will develop a one-stop shop for information on cyber security law and policy and support applied research as well as long-term endeavors in law, policy and technology.
- Developing Special Programs -- by focusing resources on certain special areas of interest, such as guidance to small business, directing cyber security knowledge and expertise directly into the homeland security discussion, integrating technological expertise with legal and policy insights to support creation of a viable underwriting market for cyber risks, and information sharing and analysis center modeling.

President Rose Delivers Keynote at NCISSE

The National Colloquium for Information System Security Education (NCISSE) recently held its sixth annual conference in Redmond, WA. The purpose of the NCISSE is to provide a forum for dialog among leading figures in government, industry and academia to work in partnership to define current and emerging requirements for information security education, and to influence and encourage the development and expansion of information security curricula, especially at the graduate and undergraduate levels. President Linwood H. Rose of JMU was invited to deliver the academic keynote address at the conference. James Madison is one of the National Security Agency's seven charter members of its "Centers of Excellence in Information Security." Following is an excerpt from President Rose's address:

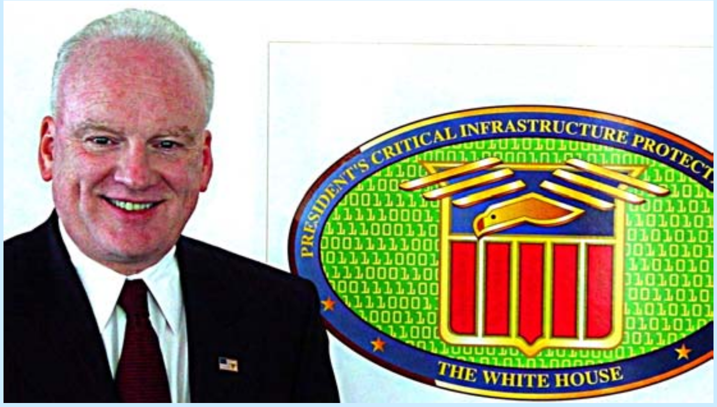
"As a university president I have awakened to a new reality: The time has come for leaders in higher education to recognize and creatively respond to the opportunity and realities that

(continued, Page 4)

*CIP LEADERSHIP HIGHLIGHT**

Richard A. Clarke

Special Advisor to the President for Cyberspace Security



Responsibilities: As the nation's cyberspace security leader, Mr. Clarke is responsible for coordinating interagency efforts to secure information systems. In the event of a disruption, he must coordinate the restoration of critical systems. Mr. Clarke works in close coordination and partnership with the private sector, which owns and operates the vast majority of America's critical infrastructure. He is the President's principal advisor on matters related to cyberspace security and reports to the Assistant to the President for Homeland Security and to the Assistant to the President for National Security Affairs. Mr. Clarke also serves as chairman of the President's Critical Infrastructure Protection Board.

Government Career: Mr. Clarke began his federal career in 1973 and has held positions such as Deputy Assistant Secretary of State for Intelligence, Assistant Secretary of State for Politico-Military Affairs, and National Coordinator for Security, Infrastructure Protection, and Counter-terrorism. He was appointed to his current position in the fall of 2001.

CIP Philosophy: We have enemies who know what they're doing, and the worst-case scenario can happen. The threats and vulnerabilities to our systems are rife, and will only continue to grow. This is a challenge that we must take seriously and treat with priority of budgets and management. There is no silver-bullet solution, but with the multitude of efforts in R&D, government procurement demands, information sharing, and cooperation between the private sector and government, we can certainly make forward progress in protecting our systems.

*Each month *The CIP Report* will highlight leaders in government, industry, and academia, providing background information on the most prominent voices in the CIP arena.

President Rose Address (continued from Page 3) protecting the national critical infrastructure provides. In order to effectively do this, it is paramount that the academy embraces and implements a vision that balances basic research with applied and integrates it into the curriculum, facilitates technology transfer, is truly interdisciplinary in program development and deployment, is engaged through strategic alliances and collaborative efforts, and balances public interest / national security with individual rights… We have an opportunity to lead.

Universities must help address the interests of society because of the legal, ethical and moral issues surrounding the complex challenge of security and individual rights. What is needed is intelligent, strategic, proactive action rather than massive and potentially oppressive reaction. We have to work to keep America open and our campuses free. We have not talked much about it during these last few days, but these are not easy issues. Our nation has more than once faced the perplexing and complicated dilemma of balancing the rights of the individual or minority against the will of a majority. James Madison, my university's namesake, was clearly fascinated with the right of majorities to rule in the governance of peoples, and he worried constantly about their abuse of that power. The rights of minorities to be secure in their liberty were his equal concern. The proper balance of the two challenged his thinking for much of his forty years in political life. In a university we have the climates and structures for the best minds to collaborate and to test one another."

Message from the Honorable John O. Marsh, Jr.

The establishment of the CIP Project as a collaboration between George Mason and James Madison Universities is a very positive step toward bringing the Commonwealth into the center of the national critical infrastructure protection agenda. The CIP Project has access to the expertise of these schools in the areas of technology, policy, and law. I believe this will result in some very substantive contributions to safeguarding our nation's critical infrastructures, and will also bring national focus onto the world class resources the Commonwealth has to offer.

I liken the CIP Project to the Prince Henry School of Navigation in fifteenth century Portugal. During that age of exploration, sailors were navigating the oceans of the world. Each expedition would report their findings back to their own country, and valuable knowledge was gained with respect to navigation, seamanship, and commerce. However, this knowledge was not widely shared. Prince Henry of Portugal recognized that by bringing these explorers together they could develop a common repository for their knowledge and findings, and thus significantly improve the system for exploration. The Prince Henry School of Navigation was the first of its kind in the world.

I believe that through cooperation between and within George Mason and James Madison, and through collaboration with government, industry, and other academic institutions, the CIP Project can also be the first of its kind, and I look forward to working with the project in the coming months.

John Marsh is the Former Secretary of the Army, and serves at George Mason University School of Law as a Distinguished Adjunct Professor and as a Senior Fellow of the Tech Center. He was recently honored by the Virginia Bar Association for his work in national security, critical infrastructure, and cyber-terrorism issues.

Brief History (continued from Page 1) security ramifications resulting from these advancements in technology. The Critical Infrastructure Working Group set forth several policy options in 1996 and the notion of protecting critical infrastructure as a national priority was born.

In July of 1996, then President Bill Clinton launched the President's Commission on Critical Infrastructure Protection (PCCIP). The PCCIP issued its findings in October of 1997 in a report called *Critical Foundations.* The report concluded that new thinking is needed to address a new breed of threats, that it is imperative to act before it is too late, and that protection of critical infrastructure can only succeed through joint efforts by all levels of government and industry. The report made a number of recommendations, many of which were reflected in Presidential Decision Directive 63 (PDD-63), *Protecting America's Critical Infrastructures*, which was issued in May of 1998.

Between 1998 and 2001, numerous CIP organizations emerged in government and industry, and CIP curricula became available at some universities. A number of significant strides were made in the areas of information sharing, outreach and education, processes for vulnerability assessments, indications, threats, and warnings, and the development of a national strategy for CIP.

The terrorist attacks of September 2001 intensified CIP efforts across the board. Although the attacks were physical in nature, the cascading damages on some sectors represented the first massive critical infrastructure attack in our nation's history. Industry and government commitment to protecting these critical systems has been redoubled, and several major initiatives have been launched in response.

At the federal level, President George Bush has made CIP a priority by forming the President's Critical Infrastructure Protection Board (E.O. 13231) and naming Richard A. Clarke to the post of Special Advisor to the President for Cyberspace Security. The latest version of the national strategy will soon be released and for the first time will include major input from the private sector. The formation of a Department of Homeland Security will have a significant impact on federal CIP initiatives. On the industry side, information sharing initiatives are expanding, and industry players are implementing emergency phone bridges, tabletop exercises, and crisis management coordination.

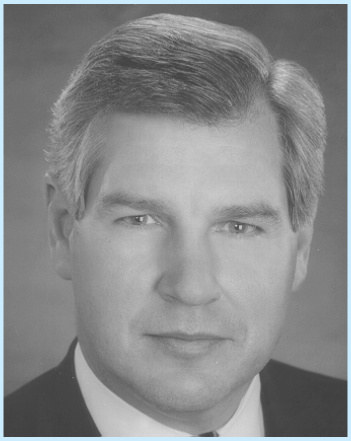
"Information technology pervades all aspects of our daily lives. Disrupt, destroy, or shut down these information networks, and you shut down America as we know it and as we live it and as we experience it every day. We need to prevent disruptions; and when they occur, we need to make sure they are infrequent, short and manageable."
Governor Tom Ridge, Assistant to the President for Homeland Security

Weblinks

Government Computer News recently published a special report called "Cyber Security: Mission Critical Now!": **http://www.gcn.com/research_results/cybersecurityhome.html**

In May 2002, the Joint Economic Committee issued a report on "Security in the Information Age": **http://www.house.gov/jec/security.pdf**

A *Washington Post* article on Al Qaeda use of cyber attacks has generated a great deal of interest in CIP: **http://www.washingtonpost.com/wp-dyn/articles/A50765-2002Jun26.html**



CEO COM Link: A Public-Private Partnership To Help Protect Our Critical Infrastructures

John J. Castellani

Leadership by chief executive offices is critical to combating terrorist threats and America's security because the private sector – not government – owns and operates most of our nation's critical infrastructures

America's CEOs have the responsibility, the ability and the desire to protect our people, our employees, our communities, and our infrastructure – and are committed to finding solutions to help the country be fully prepared to respond to a future crisis.

In a key example of a public-private partnership that will help protect homeland security, The Business Roundtable (BRT) has developed a secure telephone conferencing system that will allow the nation's top CEOs to communicate with leading government officials and each other during crises similar to the September 11th terrorist attacks.

The Critical Emergency Operations Communications Link (CEO COM Link) will be good for America. CEO COM Link is a secure telephone communications bridge that will improve the exchange of critical information between top federal leaders and the private sector in a time of crisis.

The Business Roundtable is an association of chief executive officers of leading corporations with a combined workforce of more than 10 million employees in the United States and $3.5 trillion in revenues.

CEO COM Link is one of a series of post September 11th initiatives of The Business Roundtable's Security Task Force which is chaired by Mike Armstrong, CEO of AT & T. This Security Task Force is also meeting regularly with the Office of Homeland Security and has prepared checklists and best practices on Risk Assessment and Crisis Communication.

CEO COM Link will be activated when there is a need for the federal government and CEOs to exchange information quickly, securely and efficiently.

We hope CEO COM Link is never used, but we need to be prepared. We're going to test it and make sure it will work during a national emergency, and we're all going to pray that it never has to be used.

John J. Castellani is President of The Business Roundtable.

John McCarthy is the Executive Director of the CIP Project. Please send any comments to cipp01@gmu.edu.

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.