Testimony of John A. McCarthy,
Director of the Critical Infrastructure Protection Project, George Mason School of Law
Before a joint hearing of the House Subcommittee on Infrastructure Security and
The House Subcommittee on Cybersecurity, Science, and Research & Development

September 4, 2003

Thank you, Mr. Chairman and distinguished members of the Committees for the honor of appearing before you today. I am here to testify about issues and challenges in providing for critical infrastructure protection in the context of the recent blackout and how George Mason University is assisting in this agenda.

As a preliminary matter, I'd like to introduce the Critical Infrastructure Protection (CIP) Project, within the George Mason University School of Law, where I serve as Executive Director. The CIP Project has a unique role in building an inter-disciplinary research program that fully integrates the disciplines of law, policy, and technology. We are developing practical solutions for enhancing the security of cyber networks, physical structures, and economic processes underlying our nation's critical infrastructures. The CIP Project is specifically charged with supporting research that informs needs and requirements outlined in the various National Homeland Security Strategy documents. Since its inception a little over a year ago, we have sponsored more than 70 substantive research projects, touching leading scholars at 20 universities – with James Madison University as a leading partner – and focusing more than 200 graduate and undergraduate students on security related studies. CIP Project sponsored research ranges from highly technical efforts to design new security protocols for cyber systems, to mapping the vulnerabilities of various infrastructures, to exploring the legal and business governance implications of information sharing, to experimental economic analysis of the energy sector under the direction of Dr. Vernon Smith - the most recent Nobel Laureate in economics.

In addition, GMU leads an academic consortium of regional scholars, supporting CIP vulnerability analysis and interdependency identification for homeland security planning efforts here in the National Capital Region. We are working closely with the Department of Homeland Security to ensure vulnerability assessment and modeling tools are developed locally that can be deployed nationally.

The Northeast Blackout provides a clear example of disruption to our vital infrastructures. I will focus my comments today on those issues I believe are key areas of critical infrastructure protection that require continued emphasis. These are:

- The need to develop a comprehensive understanding of infrastructure vulnerabilities and tools to assess these vulnerabilities;
- The need to better understand the complex interdependencies between infrastructure sectors; and
- The need to develop effective systems of public-private partnerships that afford true information sharing.

The Blackout and its consequences serve as an effective yardstick by which to measure critical infrastructure protection development since 9/11. On a positive note, most areas that were affected by the blackout had power restored within 24 hours. Considering the large geographic area, the number of jurisdictions involved, and the international aspects of the Blackout, this was a sound response. Particularly noteworthy were the cross-sector public-private communications that took place away from the eyes of the media. These communications involved industry, state, local and national decision-makers. I believe these relationships were not ad-hoc responses to the Blackout, but the result of the efforts of the past decade in developing a means for enhanced information exchange between the public-private sectors.

First, the Blackout experience highlights our nation's serious problems with infrastructure, including poor comprehension of our vulnerabilities and lack of awareness or preparedness for the interdependencies of infrastructures. The Blackout stresses the need to further identify, map and define our critical assets and properly assess their vulnerabilities – as have 9/11, the first bombing at the World Trade Center, Y2K, and numerous debilitating cyber attacks. Comprehensive infrastructure mapping allows us to assess exactly where vulnerabilities are, what redundancies are needed, and how to recover quickly from a disruption by physical or cyber means. It is important to map out each of the critical infrastructures, how they work with each other, and study the possible effects that the loss of one infrastructure will have on others. This type of network and vulnerability mapping is vital in addressing and managing future infrastructure disruptions. In addition, this will afford the insurance and reinsurance industries the opportunity to gather sufficient information so they can determine their appropriate role in the terrorism risk insurance arena.

These analyses must also include evaluation of myriad possible scenarios that may pose threats to critical systems and provide identification of physical and process actions, as well as economic incentives to industry that afford greater resiliency and security of key infrastructure assets. For example, in the short term, the use of redundant electrical generation at hospitals in New York City resulted in virtually no loss in service delivery capability for emergency responders and health care providers during the Blackout.

Next, the Blackout also highlights infrastructure interdependencies, which underscore the need to develop a comprehensive understanding of how these infrastructures work together. The loss of power to the energy grid implicated more than just our energy infrastructure; it cascaded into several other infrastructures. For instance, sewage piled up at a Harlem treatment plant

because there was no power to pump it through the facility. A diver had to be sent in through 40 feet of liquid sewage in order to get the pumps working again. GMU, as well as other research universities, have particular technical expertise to bring to bear in both the risk assessment of our critical assets and the advanced understanding of infrastructure interdependencies. We are fully supporting DHS's efforts to accelerate understanding in these key areas.

Finally, the interconnectivity of modern infrastructures goes beyond the technical systems themselves. The human element of critical infrastructure protection is equally, if not more important. People must communicate in order to prevent and respond to critical infrastructure failures. This high-level communication process is complex and involves many layers of connectivity. It is perhaps the most vital piece of effective infrastructure protection we can provide because we cannot anticipate every contingency. Robust information sharing must afford sufficient levels of detail at both the executive and operational levels. It should candidly identify vulnerabilities, prioritize key infrastructure assets, and allow public and private officials to prevent, respond to, and recover from potential disruptions. By the same token, sufficient safeguards and incentives must be structured for all stakeholders to fully participate in the process. As a former first responder and trained incident commander, I believe management of these complex social response networks at all levels of the federal response structure will be increasingly important in the successful resolution of infrastructure incidences of national significance, be they physical, cyber, or both. The establishment of a public-private liaison as a senior advisor to Secretary Ridge is an important and needed step in developing and advancing this emerging need.

These two Committees have chosen to address these issues at the right time, and I commend you in holding this hearing. The CIP Project's primary goal is to match scholarly

research with the real-world issues and problems faced by industry and government leaders at this important time in our Nation's history. With your continued support, the academic community can continue to provide unique fora to assist decision-makers in discussing and developing solutions to these pressing issues.

Thank you. I look forward to answering any questions you may have.