

080204  
15:15

**Testimony of John A. McCarthy**  
**Executive Director of the Critical Infrastructure Protection Program,**  
**George Mason University School of Law**  
**Before the House Committee on Government Reform**

Thank you, Mr. Chairman and distinguished members of the Committee for the honor of appearing before you today. I am here to testify about issues and challenges explored by the National Commission On Terrorist Attacks Upon the United States. In their report, the 9-11 Commission proposes bold actions that Congress and the Administration may undertake to enhance critical infrastructure protection. We believe that the recommendations, many of which this Committee has considered prior to and since the 9/11 attacks, are worthy of the Committee's time and attention.

As a preliminary matter, I'd like to introduce the Critical Infrastructure Protection (CIP) Program of George Mason University School of Law, where I serve as Executive Director. The CIP Program 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 Program is specifically charged with supporting research that informs needs and requirements outlined in the various National Homeland Security Strategy documents. The CIP Program was launched almost two years ago, since then sponsoring 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 Program sponsored research ranges from highly technical efforts to design new security protocols for cyber systems,

to mapping the vulnerabilities of various infrastructures, nationally and internationally, exploring the legal and business governance implications of information sharing, and experimental economic analysis of the energy sector under the direction of Dr. Vernon Smith, the 2002 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 with the Department of Homeland Security to ensure that vulnerability assessment and modeling tools are developed locally and are capable of national deployment.

On behalf of the Critical Infrastructure Protection Program at George Mason University, I would like to emphasize three themes today:

**First, our nation's decision to consolidate homeland security has improved information sharing in significant ways.** The Department of Homeland Security is focused and energized on sharing threat information. In providing a single point of contact, the new Department of Homeland Security is working to provide an efficient way to share threat analysis and to disseminate sensitive information -- to the right people, at the right time, and in the right manner.

The Administration's issuance of Homeland Security Presidential Directive 7 has favorably influenced information sharing initiatives. The new directive, which updates Presidential Decision Directive 63, sets expectations to share information as widely as possible, clarifies roles and responsibilities, and marshals the Administration's resources so that information sharing programs are managed effectively.

Since the 9/11 attacks, we have witnessed the private sector commit to improving security exchanges with the government in this new consolidated environment. Of course there are impediments that undermine more robust information sharing. We are, however, impressed with the relationships formed between the Information Analysis and

Infrastructure Protection directorate and the infrastructure sectors. With IA/IP's encouragement and assistance, the private sector has deployed a range of important programs and initiatives for sharing sensitive threat data – including efforts that:

1. Organized and expanded cross-sector collaboration for information sharing among critical infrastructure owner/operators in the private sector and to the government;
2. Developed an early notification system, which public and private sectors deployed this weekend surrounding the recent threat alerts;
3. Identified common physical and cyber issues for public and private sector collaboration and consideration; and
4. Identified and developed exercises related to critical interdependencies.

These could not have been accomplished prior to the 9/11 attacks.

**Second, this Committee should consider ways to involve the private sector in government-wide information sharing reforms.** Critical infrastructure owners and operators provide goods and services essential to national security, economic security, public health and safety and public confidence, the goals of Homeland Security. These owners and operators are not always treated as having a need to know. They do, however, have a compelling need for threat information.

In many cases, critical infrastructure operators are the first to respond to an incident. Industry owners and operators are, in many cases, the first line of defense. Critical infrastructures have a weighty responsibility to protect employees, service customers, and support the markets by restoring essential services from an attack quickly and effectively. These corporate responders should have access to information that Federal, State, and local responders have as well, allowing for restrictions of specifically classified information.

In this vein, we applaud the 9/11 Commission recommendations on Protecting Against and Preparing for a Terrorist attack. The Commissioners pinpoint potential areas of change, such as inclusion of private sector needs in any new national intelligence

program. We hope that this Committee will go one step further and treat private sector as inseparable from other government agencies, such as first responders and others that rely on intelligence warnings to service the public sector.

In the event the Committee decides to recommend any restructuring directives, we believe that it is important that such initiatives build upon rather than replace the initiatives already underway.

**Third, we vigorously applaud the 9/11 commissioners for promoting the critical role of technology.** Leveraging technology is critical at several levels – for analyzing substantial amounts of data, for disseminating that data, and for prioritizing who gets what, how, and when.

George Mason University, like our academic partners across the United States, is focusing research on ways to integrate technology smartly for information sharing purposes. Our priority goals at the CIPP include:

1. Developing a comprehensive understanding of infrastructure vulnerabilities;
2. Developing tools to assess these vulnerabilities;
3. Offering research on complex interdependencies between infrastructure sectors;
4. Developing concepts, metrics and models to support decisions allocating resources to homeland security initiatives and measuring their progress; and
5. Developing effective systems of public-private partnerships that afford true information sharing.

We also applaud the 9/11 Commission for recognizing the critical importance of privacy and civil liberties. One of our distinguished Professors, John O. Marsh, served on the Technology and Privacy Advisory Panel established by Secretary Rumsfeld. Prof. Marsh is now entering his fifth year of working with law students to consider new theories of privacy and ways to enhance both security and privacy rights. We encourage the Committee to consider how the 9/11 Recommendations impact existing privacy responsibilities, such as those contained in the Federal Information Security Management Act.

**Thank you. I look forward to addressing any questions you may have.**