STATEMENT OF
TY R. SAGALOW

BOARD MEMBER, FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER (FS ISAC)
CHIEF OPERATING OFFICER, AIG EBUSINESS RISK SOLUTIONS

BEFORE THE COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

MAY 8, 2002

Mr. Chairman and Members of the Committee, thank you for this opportunity to testify about the importance of information sharing in the protection of this nation's critical infrastructure. My name is Ty R. Sagalow and I come before you in two capacities today. First, as a member of the board of the Financial Services Information Sharing and Analysis Center – the FS ISAC—FS ISAC is the oldest Information Sharing and Analysis Center established as a result of Presidential Decision Directive 63, and secondly as the COO of American International Group's eBusiness Risk Solutions division, the largest provider of network security insurance in the world.

Governor Tom Ridge recently remarked:

> Information Technology pervades all aspects of our daily lives, of our national lives…Disrupt it, destroy it or shut down the information networks, and you shut down America as we know it.

The sad fact is that our information technology systems are already under attack and there is every reason to believe it will get worse before it gets better. According to a recent report of the National Research Council, U.S. companies spent $12.3 billion to clean up damages from computer viruses in 2001. Further, the report notes that 2002 could be worse. The 2002 CSI/FBI survey found that 90% of companies surveyed admitted to a successful computer breach in the preceding year resulting in hundreds of millions of dollars in quantifiable losses. Mass cyber-events such as "I Love You" virus, the Mellisa Virus and more recently Code Red and the NIMDA viruses are reported to have caused hundreds of millions, perhaps billions, of dollars in damages. Finally, the CERT organization at Carnegie Mellon reports that in 2001 they received over 50,000 incident reports, more than double of the year before which itself was double of the prior year.

Today, it would be easier for a cyber-terrorist to shut down a dam by hacking into its control and command computer network than to obtain and deliver the tons of explosives needed to blow it up. More frightening, the destruction can be launched from the safety of the terrorist's living room couch – or cave as the case may be.

We must act and we must act quickly. Fortunately, we are not powerless. Just as it is our information systems that are the subject of the attacks, it is our ability to share information which provides our best foundation for defense.

In October 1997, the *Report of the President's Commission on Critical Infrastructure Protection* identified the banking and finance sector as critical to the nation's well being. This finding was incorporated in PDD-63 in May 1998 and on October 1, 1999 at the request of the US Department of Treasury, the Financial Services Information Sharing and Analysis Center was born. Today there are over 53 financial institutions representing more than 50% of all credit assets who are members of the FS ISAC. Members include 5 of the top 10 commercial banks and 5 of the top 10 securities firms, as well as numerous insurance companies such as AIG.

The mission of the FS ISAC is straightforward: Through information sharing and analysis provide its members with early notification of computer vulnerabilities and attacks, subject matter expertise and other relevant information such as trending analysis.

We are joined in this endeavor by other organizations with similar missions. One of these is Infragard which as you know works with the National Infrastructure Protection Center (NIPC) and the private sector to create a trusted network of information sharing.

Unfortunately, I am here today to tell you that we will not succeed, we cannot succeed, in this mission without your help. Existing laws and regulations today place severe obstacles preventing the voluntary disclosure of information from the private sector to the public sector and within the private sector itself.

We believe that there are chiefly three obstacles that must be removed for effective, robust information sharing to take place. Removing these obstacles is important since companies will not disclose voluntarily if their general counsel tells them not to. And general counsels will tell them not to if there is a potential that disclosure will bring financial harm to their company. It is that simple.

As respects sharing information to the public sector, the fear exists that the competitors or others, wishing to do the disclosing company harm, will be able to obtain access to that information through the Freedom of Information Act. As respects sharing information within the private sector, there are two twin fears. First, such sharing could be deemed to be violation of either federal or state anti-trust laws and second, that the sharing of information will lead to liability against the company or its directors or officers.

The chilling effect of potential liability lawsuits on voluntary speech cannot be underestimated. Private lawsuits, or rather the fear of them, have always played an important role in fostering proper conduct. However, when applied inappropriately, they can have the opposite impact – that of chilling desirable conduct. Such is the situation here. Why disclose the potential inadequacies of a security technology when your general counsel tells you that the disclosure could lead to a defamation suit? Why recommend the use of specific technological safeguards when such disclosures could lead to lawsuits alleging tortuous interference with the contractual rights of others who use competing technology. Why freely disclose the results of millions of dollars in research and analysis of "best practices" when such disclosure could lead to shareholder lawsuits alleging misconduct in disclosing company "trade secrets" or other breaches of the fiduciary duties.

"The risk is too great." "Better to keep your mouth shut." "Better safe than sorry." These statements represent the danger that we face today fore that will be the advice given by general counsels throughout the nation. We faced this danger before, in Y2k and in Y2k we avoided it through thoughtful and balanced legislation. We must avoid the danger again.

Putting on my other hat, I can tell you that information sharing is essential to the creation of a stable insurance market for network security. Insurance plays a critical role in protecting our national infrastructure by both spreading risk among members of society as well as providing positive reinforcement for good behavior by making insurance available and affordable. *BusinessWeek* recently remarked that it will be the insurance industry which over time will influence security software standards. A working insurance industry provides a vital mechanism to structure and reward security "best practices".

Today, my company leads the way in this effort and we have already provided billions of dollars in insurance protection for thousands of companies representing all segments of our nation's infrastructure. This is but a drop in the bucket, however. Today, there are only a handful of insurance companies providing network security insurance. The reason: insurance companies cannot underwrite what they do not understand. And they cannot understand a risk if they do not have access to data on frequency and severity of risk—or at least the hope of future access to such data. Effective and robust information sharing becomes the foundation for building the actuarial tables needed to create a stable insurance industry.

In conclusion, for voluntary information sharing to be both robust and effective, the Government should take three actions:

1. Provide an exemption under FOIA for critical infrastructure information voluntarily shared from private companies or private sharing groups to the federal government,

2. Provide an exemption or guidance under the anti-trust laws on both a federal and state level to critical infrastructure information voluntarily shared in good faith within the private sector, especially within a formal structure like the ISACs, and

3. Provide safe harbor legislation similar to that provided for Y2k to protect the disclosure of critical infrastructure information within the private sector as long as such disclosure is made in good faith.

Mr. Chairman, I would like to thank the Committee for permitting me to testify today on this important subject. I would be pleased to answer any questions you might have at this time.