

**COMMITTEE ON GOVERNMENT REFORM**  
**SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,**  
**INTERGOVERNMENTAL RELATIONS AND THE CENSUS**  
**CONGRESSMAN ADAM PUTNAM, CHAIRMAN**



**April 8, 2003**

***“Cyber Security: The Challenges Facing Our Nation  
In Critical Infrastructure Protection.”***

**STATEMENT OF THE CHAIRMAN**

“Virtually every aspect of our lives is in some way, shape or form connected to computers. Networks that stretch from coast to coast, and, in fact, around the world connect these same computers to each other. In the traditional sense, we have thought of our security as a Nation in the physical...bridges, power plants, water supplies, airports, etc. Securing our physical infrastructures has been a highly visible priority, particularly since 9-11.

“The military, customs, and border patrol are charged with protecting and securing our borders. The Coast Guard protects our waterways. Federal, state, and local law enforcement protect our bridges, railways, and streets and provide for our own personal protection. However, in this day and age, this type of one-dimensional thought is no longer adequate. Our critical infrastructure, of the cyber kind, must have the same level of protection if we are to be secure as a Nation, from random hacker intrusions, malicious viruses or worse – serious cyber terrorism.

“There are several things unique to cyber attacks that make the task of preventing them particularly difficult. Cyber attacks can occur from anywhere around the globe: from the caves of Afghanistan to the war fields of Iraq, from the most remote regions of the world or simply right here in our own back yard. The technology used for cyber attacks is readily available and changes continually. And, maybe most dangerous of all, is the failure of many people -- critical to securing these networks and information from attack -- to take the threat seriously, to receive adequate training, and to take steps needed to secure their networks. I am happy to say today that all of the witnesses here today are on the forefront of this war -- on cyber terrorism -- and I’m looking forward to their insightful testimony.

“In May 1998, President Clinton released Presidential Decision Directive No. 63. The Directive set up groups within the federal government to develop and implement plans that would protect government-operated infrastructures and called for a dialogue between government and the private sector to develop a National Infrastructure Assurance Plan that would protect all of the nation’s critical infrastructures by 2003. The Directive has since been supplemented by Executive Order 13231, which established President Bush’s Critical Infrastructure Protection Board and the President’s *National Strategy for Homeland Security*.

“Since January 2001, efforts to improve federal information security have accelerated at individual agencies and at the government wide level. For example, implementation of Government Information Security Reform Act legislation (GISRA) enacted by the Congress in October 2000 was a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. In implementing GISRA, agencies have noted benefits, including increased management attention to and accountability for, information security. Although improvements are under way, recent GAO audits of 24 of the largest federal agencies continue to identify significant information security weaknesses that put critical federal operations and assets in each of these agencies at risk.

“On December 17, 2002, the Federal Information Security Management Act (FISMA) was enacted as Title III of the E-Government Act of 2002. FISMA permanently authorizes and strengthens the information security program, evaluation, and reporting requirements established by GISRA. Among its provisions, it also requires The National Institute of Standards and Technology to develop standards that provide mandatory minimum information security requirements for federal information systems.

“While securing federal information systems is critical, so is securing the critical infrastructure of the nation -- 80 percent of which is privately controlled. Reports of computer attacks abound. The 2002 report of the “Computer Crime and Security Survey,” conducted by the Computer Security Institute and the FBI’s San Francisco Computer Intrusion Squad showed that 90 percent of the respondents (primarily large corporations and government agencies) had detected computer security breaches within the last 12 months. In addition, the number of computer security incidents reported to the CERT Coordination Center rose from 9,859 in 1999 to 52,658 in 2001 and 82,094 in 2002. And, these are only the reported attacks.

“The Director, CERT Centers, operated by Carnegie Mellon University, stated, that he estimates that as much as 80 percent of actual security incidents go unreported, in most cases, because (1) the organization was unable to recognize its systems had been penetrated or there were no indications of penetration or attack, or (2) the organization was reluctant to report.

“Our own General Accounting Office has found a disturbing trend among federal agencies. In both 2001 and 2002, GAO continued their analyses of audit reports for 24

major departments and agencies. The audits identified significant information security weaknesses in each that put critical federal operations and assets at risk.

“While the federal government and private sectors have made important improvements in cyber CIP, clearly there is still much work to be done. In July of 2002 GAO identified at least 50 federal organizations that have various national or multiagency responsibilities related to cyber CIP. The interrelationship of these organizations is critical to a successful cyber CIP strategy. These federal organizations also interrelate and coordinate with even more private sector organizations as well as state and local governments.

“The ability of all these groups to communicate well, understand the risks involved, accept common goals and minimum standards, and accept full accountability will be the keys to a successful national effort to protect the nation’s critical infrastructures and our government networks.

“This Subcommittee accepts the serious nature of the oversight responsibility related to this topic, and this hearing today is just the beginning of what will be a series of hearings that examine and measure the progress towards achieving true Cyber security.”

###