Statement by
Amit Yoran
President, Yoran Associates
Former Director, National Cyber Security Director,
Department of Homeland Security
"HR 285: The Department of Homeland Security
Cybersecurity Enhancement Act of 2005"

Before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity
Committee on Homeland Security
U.S. House of Representatives
April 20, 2005

Good afternoon, Chairman Lungren and distinguished Members of the Subcommittee. My name is Amit Yoran and I am pleased to have an opportunity to appear before the subcommittee today to discuss enhancements to our national efforts to security cyberspace. I am the President of Yoran Associates, a technology strategy and risk advisory business headquartered in Northern Virginia. In our practice, we advise a number of global enterprises on their technology strategy and associated business risks and exposures. Prior to founding Yoran Associates I served as the Director of the National Cyber Security Division of the Department of Homeland Security (DHS), responsible for building, 1) a national cyber response system; 2) a national threat and vulnerability reduction program; 3) a national cyber awareness and training program; and 4) establishing increased security and coordination among and between government and international counterparts. Much work has been done in the implementation of the above responsibilities by both the public and private sector and even more work remains ahead of us.

Protecting America from physical threats is a concept well understood by senior leadership and risk managers, where sound understanding of the challenges, consequences of failure, and specific work plans to be accomplished are ongoing as part of a unified protection effort. Our ability to conceptualize and defend against physical threats has matured over many years. Changes to critical infrastructures do not occur on a highly dynamic basis. On the other hand, our use of and reliance on technology transforms continually in modern competitive environments . Significant challenges remain in raising awareness and understanding of vulnerability to cyber failures or attacks to the leadership which structure and resource defensive efforts. This challenge to change our thinking is consistent in government and the private sector.

Since the creation of the Department of Homeland Security, approximately two years ago, a massive restructuring has occurred in the Federal Government. But more important than the restructuring and the organizational charts is the fantastic work being accomplished by so many talented and dedicated public servants serving in the most noble and challenging undertakings; protecting our homeland and the American people.

The task in securing America's cyber infrastructures is a daunting and very real challenge. Efforts to secure the computer systems on which our nation's critical infrastructures and our economic stability rely are being addressed with a pre-9/11 lack of urgency. As we failed to grasp the gravity of the World Trade Center bombings in 1993, today we are not acting aggressively on the numerous warning signs of critical infrastructure computer failures; the Northeast-Midwest blackout of 2003, ATM outages and airline system failures or on the numerous computer threats actively working against our economic security. Simply put, many American business interest have a significant if not complete reliance on general purpose computers and inter-connected networks which can generally be categorized as untrustworthy. The recipes for disaster are present.

Responsibility for protecting these business critical systems lies largely in the private sector where nearly all of these critical infrastructure systems are owned and operated. Organizational leadership must encourage the inclusion of technology risks into their business risk management practices. Responsible business risk practices require a thorough evaluation and informed acceptance of technology and business exposures or investment in risk mitigation techniques. Forward thinking organizations are protecting themselves from significant threats and exercising their response plans in simulated cyber crisis scenarios. These types of activities can be used to effectively create awareness among organizational leadership. In essence, industry must not wait for government action to begin securing systems and improving organizational policies and procedures.

Some critical functions and responsibilities in our national cyber security efforts are inherently governmental, such as providing a survivable communications capabilities in various bad-case cyber and telecommunications outage scenarios, raising awareness of threat information and coordinating national response efforts. I challenge the Committee to assist the Department in increasing the investments being in fundamental cyber security research and development.

Secretary Chertoff is in the midst of his departmental analysis and restructuring effort – the second stage review. The Directorate of Information Analysis and Infrastructure Protection under which the National Cyber Security Division resides, is charged with performing some of the most important mission functions of DHS. It is imperative that we afford the Secretary the opportunity to design and structure the Department to the best of his ability and satisfaction and to provide him and his team whatever support we can in accomplishing their mission. Creating greater unity and clarity around cyber efforts will result in the further inclusion and better integration of cyber security thinking, awareness and protective measures across all of the various programs and efforts taking place to protect America.

The creation of an Assistant Secretary position to address cybersecurity issues is not inconsistent with a unified or integrated risk management approach. On its own it does not address the Government's challenges in cyber security. There are several areas where greater clarity is needed and support must be given to centralize cyber security functions across government. The Department of Homeland Security struggles with its mission responsibilities of security for government computer systems, but FISMA authorities lay entirely within OMB.

Consideration of this topic by the Committee can provide needed attention and have significant impact on improving operations and government cyber preparedness. Procurement practices by the Federal Government to enhance cyber security features, functionality and requirements are not effective and are rarely enforced with consistency, resulting in the single greatest missed opportunity to positively influence and drive better security capabilities into the product sets used by both government and private sectors.

There are many dedicated Americans in both the public and private sector working on these challenges our economic and homeland security. It is my hope that this Committee on Homeland Security can provide them further mission guidance, support our common cause and assistance wherever possible. I look forward to answering any questions you may have.