National Strategy for Homeland Security -POTUS

Letter, Oct 5, 2007 – New Emphasis on Cyber Security

- ❑ *A variety of actors threaten the security of our cyber infrastructure.* ***Terrorists increasingly exploit the Internet to communicate, proselytize, recruit, raise funds, and conduct training and operational planning. Hostile foreign governments have the technical and financial resources to support advanced network exploitation and launch attacks on the informational and physical elements of our cyber infrastructure.***

- ❑ *In order to secure our cyber infrastructure* ***against these man-made and natural threats, our Federal, State, and local governments, along with the private sector, are working together to prevent damage to, and the unauthorized use and exploitation of, our cyber systems.***

Cyber Security; Government and Industry Best Practices Panel Members

Dr. Tommy Augustsson, CIO General Dynamics,
taugusts@generaldynamics.com, 703-876-3473

Mr. Jerry Cochran, Principal Security Strategist, Microsoft
Jerry.Cochran@microsoft.com

Mr. Richard Hale, Chief Information Assurance Executive, DISA
Richard.hale@disa.mil 703-882-1500

Dr. Mark Thomas, Senior Advisor, Army DIB Task Force
Mark.Thomas2@us.army.mil 703-697-9424

Mr. L. Rick Anderson, Dep, Dir DIB Cyber Security Task Force
Levon.Anderson@osd.mil 703-604-5523, ext 123

Cyber Security; Government and Industry Best Practices Panel

What are some of the major partnership challenges between DOD and Industry as related to cyber security info sharing and reporting? Provide possible or proven solutions if applicable (e.g., technology, procedural, regulatory, etc...).