EMBARGOED FOR RELEASE ON MARCH 18,2004 AT 2:00 PM EASTERN

Awareness and Outreach Task Force
Report to the National Cyber Security Partnership
March 18, 2004

Executive Summary

About the Task Force

The Awareness and Outreach Task Force, an industry-led coalition of interested security experts from the public and private sectors, was created as part of the National Cyber Security Summit process. Task force members include representatives from trade associations, nonprofit organizations, publicly traded and privately held companies, and state, local, and federal government. Task force members participated voluntarily, donated their time, and were not paid.

The task force is not an advisory group to the Department of Homeland Security (DHS) or any other state, local, or federal government department or agency. Instead, it operates under the guidance and coordination of the National Cyber Security Partnership, a coalition of trade associations, including the U.S. Chamber of Commerce, the Information Technology Association of America, TechNet, and the Business Software Alliance, that sponsored and organized the National Cyber Security Summit held in Santa Clara, California, on December 2—3, 2003.

TASK FORCE MISSION

Originally, this task force was charged with developing an awareness campaign to inform small businesses and home users about the importance of cyber security. However, during the December 2--3, 2003, National Cyber Security Summit, the task force expanded its scope beyond small businesses and home users to more accurately reflect the priorities of the *National Strategy to Secure Cyberspace*. The current mission and description of the taskforce follows:

Mission: To promote a comprehensive national awareness program to empower all Americans—businesses, the general workforce, and the general population—to secure their own parts of cyberspace.

Description: The Awareness and Outreach Task Force has developed implementation strategies and tactical plans that target home users, small businesses, large enterprises, schools and institutions of higher education, and state and local governments. Recognizing that we all have a role to play, each constituency has provided practical steps to increase awareness, accountability, and understanding to take action to manage the risks we face in today's constantly changing environment.

Task Force Co-Chairs:

- Dan Caprio, Chief of Staff to Commissioner Orson Swindle, Federal Trade Commission
- Ty Sagalow, Worldwide Corporate Product Development, Deputy Chief Underwriting Officer and DBG-Vice President, American International Group and COO, AIG eBusiness Risk solutions.
- Howard Schmidt, Vice President and Chief Information Security Officer, E-Bay, Inc.

The U.S. Chamber of Commerce serves as the Task Force Secretariat. The Task Force Co-Chairs thank Andrew Howell, Vice President for Homeland Security, and Scott Algeier, Manager for Homeland Security, both at the U.S. Chamber of Commerce, for their significant contributions to this report.

PROBLEMS and CHALLENGES

- Although the Internet has increased communication and productivity has provided businesses with access to new markets, it has also given hackers, thieves, disgruntled employees, fraudsters, and other criminals new opportunities to cause economic and social damage on a broader scale and has created new potential weapons of terrorism, more quickly than ever before.

- Generally, many private enterprises, public entities, and home users lack the resources to adequately manage cyber security risk.

- A large number of entrepreneurs and home users are not aware of how their individual cyber security preparedness affects security overall.

- Internet users must be made aware of the importance of sound cyber security practices and given more user-friendly tools to implement them.

RECOMMENDATIONS and NEXT STEPS

Small Businesses

- Develop and distribute a cyber security guidebook for small businesses and encourage the development of market-based incentives such as insurance and risk profile analysis that reward small businesses that enhance their cyber security preparedness.

Home Users

- Support, promote, and launch a national public service campaign on cyber security.

- Develop a cyber security tool kit for home users.

- Work with the Internet Service Provider (ISP) communities to identify ways to use their access to their customers to promote cyber security.

Large Enterprises

- Create and implement, in September, 2004, in partnership with DHS, a series of regional homeland security forums for CEOs of large enterprises. A portion of the program should highlight the roles of CEOs in cyber security.

- Begin, in July 2004, a direct mail campaign to C-Suite executives of the 10,000 largest companies in America to provide senior corporate executives with key messages and activities that are necessary for enterprisewide cyber security.

- Designate September 2004 as Cyber Security Month, and market to CEOs of large enterprises the importance of focusing on cyber security and participating in the DHS CEO regional homeland security forums.

- Distribute and raise awareness of the cyber risk management tools being developed by the Cyber Security Summit's Corporate Governance Task Force.

K-12 Schools and Higher Education

- Inventory, catalogue, and share best practices on raising cyber security awareness to home users, large enterprises, small businesses, K—12 schools and institutions of higher education, and state and local governments.

- Partner with education groups, school boards, superintendents, teachers, and colleges and universities to develop and distribute materials to school children and institutions of higher education that raise awareness of appropriate cyber security behavior.

- Provide cyber security and ethics curricula and explore opportunities for introducing awareness content as part of courses.

- Consider replicating the DHS Homeland Security CEO Forums for university presidents. A portion of the program should highlight the roles of university presidents in cyber security.

State and Local Government

- Develop, in conjunction with DHS, a Cyber Security Excellence Award to recognize teams, rather than individuals, at the state and local government levels.

- Create a Web-based training tool for state and local governments, as well as for businesses and home users, featuring a series of webcasts hosted by a variety of vendors, which are offering their services pro bono.

- Consider replicating the DHS Homeland Security CEO Forums for governors. A portion of the program should highlight the roles of governors and mayors in cyber security.

CONCLUSIONS

A major role for the Awareness Task Force has been, and will continue to be, to leverage existing awareness and outreach efforts and to initiate and enhance public-private partnerships. Promoting a secure cyberspace is the responsibility of every citizen, all levels of government (state, local, and federal), academia, and industries, regardless of size or sector. The list of key stakeholders involved in the solution is limitless, and therefore, the solution will only come as a result of coordinated, public-private partnerships.

The progress of the task force demonstrates the effectiveness of the public-private partnership model. Task force members believe that more can be accomplished

by working together, rather than by working separately. The task force has catalogued existing best practices, developed strategies to market those practices to specific audiences, created incentive plans to ensure acceptance of those practices, contributed to the development of a national advertising campaign, and developed a strategy to communicate to public and private CEOs across the country about the importance of cyber security and their role in enhancing it. Recognizing the role of our students, teachers, and schools and universities, a strategy has been created to bring cyber security directly to them. In addition, the task force has a team of dedicated state and local public servants who have taken shared responsibility in enhancing cyber security awareness in state and local government agencies throughout each state.

While these accomplishments are extensive, the task force recognizes that there is much more to do. The task force also acknowledges that there are other groups who are making positive contributions to cyber security awareness and encourages interested parties to comment on this report and join in the task force's efforts.