# National Early Warning Task Force Recommendation

## A NATIONAL EARLY WARNING CONTACT NETWORK

## EXECUTIVE SUMMARY

### About the Task Force

The Early Warning Task Force (EWTF) is an industry-led coalition of interested security experts from the public and private sectors created as part of the National Cyber Security Summit process. Task force members include representatives from trade associations, non-profit organizations, publicly traded and privately held companies and state, local and federal government employees. Task force members participated voluntarily, donated their time and were not paid for their participation. The task force is not an advisory group to the Department of Homeland Security or any other state, local or federal government department or agency. Instead, the task force operates under the guidance and coordination of the National Cyber Security Partnership, a coalition of trade associations comprising 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

The mission of the EWTF is to improve the sharing, integration and dissemination of information about cyber security threat, vulnerabilities, exploits and incidents at organizational and human levels (e.g., ISAC's and cyber security professionals), within a vetted trust community.

The EWTF has also considered implementation objectives for the recently announced US-CERT to: 1) improve warning and response to incidents; 2) increase coordination of response information; 3) reduce vulnerabilities; and 4) enhance prevention and protection efforts.

### PROBLEM/CHALLENGE

The EWTF identified its problem statement as:

*How do we effectively identify and gather cyber-warning information, analyze the information and communicate the correct warnings to the right people in a timely manner.*

### RECOMMENDATIONS FOR A NATIONAL EARLY WARNING CONTACT NETWORK

- Create a National Cyber Security Early Warning Contact Network (EWAN)

- The primary goals are to broaden the horizon of shared information regarding cyber security vulnerabilities, exploits and incidents, to facilitate the process of information sharing and to provide a facility for the rapid dissemination of critical information, all within the framework of a vetted trust community.
- EWAN will be a multi-channel communications network housed and administered in the US-CERT.
- EWAN will include high-level guidance or protocols, in consultation with DHS/US-CERT, for the types of information required to generate an "early warning alert" and for potential sector or functional subgroups needed for a particular action or response.
- EWAN will reflect the 14 critical infrastructure sectors identified in HSPD-7, and the established and developing sector representations and information-sharing organizations.
- EWAN is not intended to replace existing communities that act for cyber defense and response, but rather, to serve as a complementary means to promote secure public/private collaboration.

**NEXT STEPS**

- The Early Warning Task Force seeks public comment on these preliminary recommendations for the EWAN as set forth in the main report. Commenters are asked to consider the recommendations as posed, as well as provide specific suggestions for implementing the design and management of the network in order to bring it into operation as soon as possible, with ongoing refinements as experience dictates.
- The Department of Homeland Security should facilitate the ongoing discussion among stakeholders such that the network provides maximum value to all the communities, both individually and ecumenically.
- Following an eight-week comment and consideration period, the Early Warning Task Force organizers will prepare an updated report in June 2004 to reflect stakeholders' input.