

National Early Warning Task Force Recommendation

A NATIONAL CRISIS COORDINATION CENTER

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 CRISIS COORDINATION CENTER

Create a National Crisis Coordination Center to:

- House government, industry and academic security experts, both physical and cyber, to bridge the cultural barriers that have hampered a true partnership in counterterrorism and cyber security
- Jointly prepare, exercise, evaluate and update National Joint Crisis Response plans to prevent, detect and respond
- Operate joint watch centers
- Conduct joint exercises at the national level to train and test the plans
- Conduct joint field training at the regional level to train and further test the plans
- Respond jointly to traditional natural events, as well as malicious events
- Proactively share intelligence – both national security and law enforcement
- Include a secure, compartmented intelligence facility staffed equally with government and private sector representatives, as well as appropriate state, local and other representation
- Proactively address priority remediation of systemic vulnerabilities in national level infrastructures

NEXT STEPS

Development of consensus around an NCCC model as described will require input from all stakeholders, including federal agencies, Congress, the private sector, law enforcement and state and local governments. This process will take some time, but Congress should consider concerted inquiries into the concept during 2004, with deliberations continuing in 2005 to result in a workable concept, either through authorizing legislation for funding and/or executive order.