Frequently Asked Questions
National Cyber Security Partnership
Early Warning Task Force
March 17, 2004

What is the Early Warning Task Force?
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 is also working with the US-CERT and Department of Homeland Security to improve warning and response to incidents; to increase coordination of response information; reduce vulnerabilities; and enhance prevention and protection efforts.

What companies and organizations have been involved in the task force?
The Information Technology Association of America (ITAA) serves as secretariat for the task force. Task force chairs are: Guy Copeland, Vice President, CSC; Suzanne Gorman, SIAC; and Rich Pethia, Carnegie Mellon University; Other companies and organizations participating are:

- Accenture National Security Services
- ArcSight
- BearingPoint
- Bell South
- BITS/Financial Services Roundtable
- Computer Associates
- FS/ISAC
- Hewlett Packard Company
- House Select Committee on Homeland Security
- Indiana University
- Intel Corporation
- Internet Security Systems, Inc
- Microsoft
- NASCIO
- Network Associates Inc.
- NYS Cyber Security and Critical Infrastructure
- Phoenix Technologies
- Preventsys
- Qualys
- SAIC
- SBC Internet Services
- Sigaba
- Sprint
- SRA
- Stanford University Medical Center
- Symantec Corp

- System Design Laboratory, SRI International
- TeleCommunication Systems, Inc
- The MITRE Corporation
- US Military Academy
- VeriSign

Why is early warning important to cybersecurity?

The best approach to cybersecurity is to identify and prevent attempts to spread worms and viruses or to gain unauthorized system entry. Hackers often probe for security weak spots before finding an "open door," share attack tools, brag about exploits in open forums, operate in a predictable manner or seek out targets that fit a particular pattern. As a result, by sharing information, attacks can be predicted, analyzed and their affects mitigated through concerted action. Early warning networks provide a channel for this activity. Unfortunately, previous attempts to build these networks have been hampered by the unwillingness of participants to share information on a timely basis, to share across industries and with government agencies, to know exactly what information to share, and other issues. The Task Force has recommended creation of an Early Warning Alert Network to serve as a "network of early warning networks" and act as two-way conduit of information among critical industry infrastructure sectors.

How will EWAN operate?

EWAN will maintain multiple channels of information for situational communications, alerts, analysis and emergency coordination. Situational communications will be disseminated on a daily basis. The alert information channel will provide a means to distribute alerts with actionable information of a timely nature. The analysis communications channel will provide a secure means for cyber security analysts to exchange and coordinate analysis with the DHS/US-CERT and National Crisis Coordination Center. The call coordination channel will allow short lead time conference calls. EWAN will also operate a secure portal.

How will EWAN be funded?

Under this proposal, the EWAN will be operated under the auspices of the US-CERT, which receives funding from the Department of Homeland Security. "In-kind" funding occurs through stakeholders' participation in and allocation of staff resources to the network and the private-sector representation in the governing structure.

How is EWAN different from the recently announced DHS National Cyber Alert System?

The National Cyber Alert System is a "one to many" system, distributed by the federal government to individual subscribers. The EWAN is a "many to many" system. Information flows in the EWAN network will move back and forth between participants, with information exchange performed on a voluntary basis. EWAN participants will be composed of backbone and network service providers, technology vendors, online businesses, information sharing and analysis centers, sector coordinators, research and academic groups and government agencies. EWAN is being designed to complement, not compete with or replace existing early warning systems.

How many sectors will participate in EWAN?
Current plans call for the participation of 14 critical infrastructure sectors.

What challenges remain to implementing EWAN?
Several issues remain to be worked through the task force, including common agreement on the protocol for posting information, the designation of recipients for such information, and rules for information storage, handling and disposal.

When will the EWAN go live?
Beta testing of an EWAN development environment is slated for April 30, 2004, with launch of the production version in December, 2004.

Why did the task force recommend a National Crisis Coordination Center?
Although various information sharing and crisis coordination centers already exist, including the Department of Homeland Security's National Homeland Security Operations Center and US-CERT, a single physical center that pulls together public and private sector constituencies for full crisis prevention and response coordination seems to be missing. The NCCC would be the resource whereby stakeholders could perform advanced planning and testing of response capabilities and form a true, trust-based public/private partnership.

Would the NCCC be a physical structure?
Yes. The task force recommends a government provided facility with large crisis coordination operations center, equipped with collaboration tools, backup power, a backup hot site and other resources.

Who would staff the NCCC?
The NCCC would be staffed by representatives contributed from each critical infrastructure, appropriate federal departments and agencies, state and local governments, and first responders.

What would this staff do during non-crisis periods?
The NCCC staff would prepare, exercise, evaluate and update crisis response plans, conduct joint exercises at the regional and national levels to test plans, engage in joint intelligence sharing with national security and law enforcement agencies, and address systematic vulnerabilities in national infrastructures. The NCCC could also be used for research, best practices collection, and the training of others at the national, regional, state, and local levels.