National Early Warning Task Force Recommendation

A NATIONAL EARLY WARNING CONTACT NETWORK

About the Task Force

The Early Warning Task Force 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 Description, Problem Statement and Objectives

The Early Warning Task Force (EWTF) is one of five task forces established during the National Cyber Security Summit to address fundamental areas where private and public cooperation can result in overall improvements to cyber security. 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.*

Guided by the problem statement, the EWTF identified objectives 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.

Implementation of the EWTF's recommendations will also inform operational objectives for the recently announced US-CERT, established by the Department of Homeland Security (DHS), to: 1) improve warning and response to incidents; 2) increase coordination of response information; 3) reduce vulnerabilities; and 4) enhance prevention and protection efforts.

Relevant Guidance in National Strategy to Secure Cyber Space

The EWTF tracks with Priority #1 of the National Strategy, which calls for a "National Cyberspace Security Response System." The EWTF focused on one element of a response system: a contact network through which to distribute critical information in a timely way, such that it serves early warning to prevent or mitigate the impact of cyber security incidents. Specifically, the National Strategy encourages the "Development of a Private Sector Capability to Share a Synoptic View of the Health of Cyberspace":

> *The lack of synoptic view of the Internet frustrates efforts to develop Internet threat analysis and indication and warning capabilities. The effects of a cyber attack on one sector have the potential to cascade across several other sectors, thereby producing significant consequences that could rapidly overwhelm the capabilities of many private companies and state and local governments. ...*
>
> *Separately, industry is encouraged to develop a mechanism – whether virtual or physical – that could enable the sharing of aggregated information on Internet health to improve analysis, warning, response and recovery. To the extent permitted by law, this voluntary coordination of activities among nongovernmental entities could enable different network operators and Internet backbone providers to analyze and exchange data about attacks. Such coordination could prevent exploits from escalating and causing damage or disruption of vital systems.*

Key Stakeholders and Interdependencies

Early warning is necessary for the protection of networked devices from cyber threat. End-users, system administrators and executives all require a timely flow of information to protect and properly manage their domains. Types of required information vary, as do information disclosure protocols. Key stakeholders identified for EWTF product are those groups entrusted to manage information flows and systems, protect critical sectors and provide for cyber security, including:

- Backbone and network service providers
- Security technology and service vendors
- Online businesses
- Information sharing and analysis centers
- Critical infrastructure sector coordinators
- Research and academic groups
- Federal, state and local governments

- Associations supporting the work of the aforementioned groups

Inventory of Related Industry-Focused Work Programs or Products

a) US-CERT and CERT/CC, Carnegie Mellon University: Analyzes the state of Internet security and conveys that information to system administrators, network managers and others in the Internet community.

b) National Coordinating Center for Telecommunications (NCC): The NCC has served as the focal point for crisis coordination, disaster response and information sharing for the telecommunications industry since 1984. Major telecommunications carriers and equipment operators share information about threats, vulnerabilities and cyber-incidents regularly.

c) Infraguard: Launched in 1996 to fight cyber and physical threats to critical infrastructures; composed of 80 local chapters with industry and FBI representatives. Information sharing is characterized as more effective at local level but less so at national level because of concerns about FOIA.

d) ISACs: Established by PDD 63 in 1998, Information Sharing and Analysis Centers share information on vulnerabilities, threats and breaches within specific sectors, such as water, transportation, energy, IT, etc. These have varying levels of interest in and effectiveness of cyber security information sharing.

e) GEWIS: The Global Early Warning Information System, established in October 2003, is a program operated by DHS to measure traffic flow, latency and activity on the Internet and reports potential cyber attacks or disruptions to the government. The focus of the program is on monitoring network performance rather than content.

f) CWIN: The Cyber Warning Information Network, a vehicle for government and business to coordinate during a public network outage over a secure network, is designed to link about 75 network operations centers in the United States, 60 of which belong to the private sector.

g) CIDDAC: The Cyber Incident Detection and Data Analysis Center involves an alliance of end users, vendors and the Philadelphia Chapter of Infraguard to overcome industry resistance to information sharing by automating the delivery to the government of nonproprietary data on attacks and trends.

h) CEO COM Link: The Critical Emergency Operations Communications Link, created by the Business Roundtable, allows business and government to trade information over a secure dial-up network on imminent threats for the purpose of response and recovery.

i) BITS/FSR Crisis Communicator is used by members of BITS, The Financial Services Roundtable and the Financial Services Sector Coordinating Council (FSSCC) to contact key industry players in the

financial services industry, other sectors, financial regulators and other government agencies (where appropriate) via e-mail, telephone, cell phone, fax and pager in the event of an emergency.

j) Network Security Information Exchanges (NSIEs): Sponsored by DHS, the Government NSIE and the Industry NSIE are comprised of government and telecommunications industry representatives who meet every other month to discuss threats, vulnerabilities and cyber-security issues in a confidential, trusted environment.

k) Forum of Incident Response and Security Teams (FIRST): This coalition brings together a variety of computer security incident response teams from government, commercial and academic organizations with the aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents and to promote information sharing among members and the community at large.

l) NSP–SECURITY: The NSP-SEC forum is a volunteer incident response mailing list, which coordinates the interaction between ISPs (Internet Service Providers) and NSPs (Network Service Providers) in near real-time and tracks exploits and compromised systems as well as mitigates the effects of those exploits on ISP networks.

m) Department of Energy Computer Incident Advisory Capability (CIAC): CIAC provides advisories and alerts via e-mail, with on-line web notification in development. For severe warnings, CIAC provides an emergency contact phone tree.

n) ITAA Sector Coordinator Contact Network: As part of its responsibility as Sector Coordinator for the information technology sector, ITAA maintains an email-based contact network of approximately 1,400 individuals in the IT sector, many of whom have further reach into their trade association and trusted community memberships. Information traveling over the network involves both cyber security alerts and other critical infrastructure alerts initiated by the Department of Homeland Security through its Executive Notification System.

o) Sector Coordinators: Some critical infrastructure sectors have established private sector coordinators to foster and facilitate coordination of sector participants, other sectors and the government. For example, the financial services sector established the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). The objectives of the FSSCC are to provide broad industry representation for CIP/HLS and related matters for the financial services sector and for voluntary sector-wide partnership efforts; foster and promote coordination and cooperation among participating sector constituencies on CIP/HLS related activities and initiatives; identify voluntary efforts where improvements in coordination can foster sector preparedness for CIP/HLS; establish and promote broad sector activities

and initiatives that improve CIP/HLS; and identify barriers to and recommend initiatives to improve sector-wide voluntary CIP/HLS information and knowledge sharing and the timely dissemination processes for critical information sharing among all sector constituencies. The Council works closely with the Treasury Department, the supporting government agency for financial services critical infrastructure protection and the Financial and Banking Information Infrastructure Committee (the public-sector equivalent), which Treasury chairs. The ISAC for the financial services industry — FS/ISAC — provides operational services relative to information dissemination and anonymous sharing of incidents, threats and vulnerabilities for the sector and is a separate entity from the FSSCC. Whereas the FSSCC focuses on the strategic coordination efforts for the financial services sector, the FS/ISAC focuses on operations relative to information dissemination and anonymous sharing of incidents, threats and vulnerabilities within the sector.

p) Other Technical Sources: Information is often shared in settings that are aimed at the network security community. Examples include DShield.org, Incidents.org, NANOG and other technical and commercial bodies focused on cyber security.

Recommendations for New Initiatives and Expected Outcomes

To achieve the stated objectives of the EWTF, our recommendation is to create and maintain a national cyber security early warning contact network, named here as the Early Warning Alert Network, and herein referred to as EWAN. Certain principles of the concept include:

a) 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.

b) The goals will be achieved via the creation and maintenance of a trust community and supporting cyber systems and networks.

c) EWAN will minimally support intra-private sector information sharing, i.e., information that does not pass to government, and sharing that includes private sector and government entities, and may support the sharing of information with government that can be guided by the proposed Protected Critical Infrastructure Information Program.

d) EWAN must be fail-safe in the face of a debilitating attack on public and private Internet infrastructure. Primary EWAN traffic will be carried on Internet infrastructure, and alternative, backup methods for disseminating critical information will be provided.

e) The trust community will be established as a meta-network of vetted existing and developing trust communities, such as ISACs and cyber security defense and response organizations and communities, which have member-vetting processes that meet minimum EWAN standards.

f) Reach within the constituent trust communities is incumbent upon those communities. The EWAN administrators will provide processes, tools and marketing to aid the communities in establishing reach.

g) EWAN will reflect the key critical infrastructure sectors and the established and developing sector representations and information sharing organizations.

h) EWAN should, to the maximum extent feasible and appropriate, incorporate involvement from the information sharing networks described in *Inventory* (above) and other government sources, including DHS/US-CERT, FedCIRC, DOD-CERT and others.

i) EWAN is not intended to replace existing communities that act for cyber defense and response, e.g., FIRST, NSP-SEC, etc., but rather to serve as a complementary means to promote secure public/private collaboration.

j) 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 potential sector or functional subgroups needed for a particular action or response.

k) The EWAN governing structure will be composed of private sector and government representation.

l) The protocols for use of the network will be formalized by MOU among the participants.

m) A single point of focus, such as the role played by DHS/US-CERT, is critical for effective coordination of this effort.

Specific Requirements and Recommendations

The scope of this document is to establish a framework for further development of detailed requirements and recommendations for EWAN. The process to define those specifics will begin and progress according to the timeline described in *Key Deliverables and Timeline*. For purpose of illustration, a few ideas discussed regarding possible specific requirements and recommendations include:

a) Multiple channels of sensitive, not-for-public-release information will be supported, including i) situational communications; ii) alert; iii) analysis; and iv) emergency call coordination:

   i. The situational communications information flow contains concise daily summary reports on current cyber security situation. The reports are the output of collaborations of cross-sector, cross-organizational,

private and governmental entities that engage in daily situational interaction.

ii. The alert information channel provides a means to distribute alerts that contain actionable information of a timely nature intended to elicit immediate community response.

iii. The analysis communications channel provides a secure means for cyber security analysts to communicate regarding analysis activities, and provides a channel for information to be communicated to DHS/US-CERT and the National Crisis Coordination Center.

iv. The call coordination channel provides facility to coordinate short lead time conference calls in reaction to alerts or threat. Notifications are distributed via secured communications on the commercial Internet and via messaging to phones, pagers, SMS, etc.

b) As the concepts for EWAN and other similarly purposed DHS systems evolve and their respective requirements are identified, EWAN may be established as a distinct system, or EWAN requirements may inform the development of the other DHS systems.

c) US-CERT should initially coordinate with the DHS Infrastructure Coordination Division to develop an appropriate administrator function to reach all sectors through sector coordinators and ISACs.

d) EWAN may support horizontal segments along functional levels, such system administrators, VP operations and/or security and C-Level executives.

e) A standard method for describing alert information will be employed, including information tags for community of interest, public disclosure and criticality.

f) Each sector and community can set specific information sharing protocols in their own community, respecting guidelines established by EWAN for member vetting and public disclosure.

Key Deliverables with Timelines

A development environment and production deployment of EWAN will proceed according to:

a) Deliverable Timelines

i. Requirements definition will be completed June 30, 2004.

ii. Beta testing begins October 1, 2004

iii. Outreach to relevant communities begins October 1 to prepare for a production EWAN launch on December 3, 2004.

iv. All sectors will be invited to participate in a trial exercise prior to launch to test the functionality of EWAN and enhance its utility.

v. The EWAN implementation team will complete outreach to 100% of the key critical infrastructure sectors by December 3, 2004, on the first anniversary of the National Cyber Security Summit

b) Lead Organization(s) Responsible for Each Deliverable

i. DHS/US-CERT in cooperation with the EWTF will form a Working Group composed of private sector and government representation, charged with the responsibility to identify the detailed and specific requirements for EWAN; and will provide subsequent analysis regarding the compatibility of EWAN and other similar DHS initiatives.

ii. DHS/US-CERT will provide potential users of EWAN a feedback channel through the establishment of regular meetings, conferences, etc., to advise the Working Group on requirements, administration and operation.

iii. DHS/US-CERT will house and maintain EWAN with financial and other support from DHS and private sector participants.

iv. DHS/US-CERT will develop an exercise to be staged prior to release of the full program to test the utility of EWAN capability.

v. DHS/US-CERT will work with sector coordinators and ISACs to develop programs to extend the reach of EWAN within the respective sectors.

c) Resource Requirements and Recommended/Committed Sources

It is anticipated that the administration of EWAN will be managed and supported by DHS/US-CERT, with strong collaboration from public and private organizations.