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.

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

Task Force Report

INTRODUCTION

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.

WORKING GROUPS

Because of the diversity of each target audience, the task force established five working groups to develop plans to target specific audiences. The working groups and their chairs are as follows:

Home Users: Tiffany Jones, Manager, Government Affairs Symantec Corp.
Small Businesses: Kai Tamara Hare, Chief Executive Officer nuServe[SM]
State and Local Government: Will Pelgrin, Director, Office of Cyberspace Security and Critical Infrastructure Protection, State of New York
Large Enterprises: Marc Jones, President and Chief Executive Officer, Visonael
Higher Education and Schools: Jim Tiecher, Executive Director, Cyber Smart and Rodney Petersen, Policy Analyst and Security Task Force Coordinator, EDUCAUSE

THEMES OF THE AWARENESS CAMPAIGN

Each working group developed action plans based on these themes:

Explain the problem. Successful awareness programs need to explain to the constituents what the problem is and why cyber security is important.

Promote Individual responsibility. All people have a role to play and need to understand the importance of being proactive.

Motivate. Constituents need to be motivated to implement cyber security steps that will ultimately change behavior (positive and negative reinforcements).

Keep it simple. Cyber security needs to be simple for users to implement.

Be creative. Policymakers and industry representatives need to be creative when thinking about cyber security issues, possible actionable steps, and matrixes to measure results.

Leverage existing programs and relationships. Reaching out to industry is a quick and easy for "spreading the message" about cyber security awareness.

SELECT ACCOMPLISHMENTS TO DATE

Small Businesses

Tools for Small Businesses

- Developed, with the Internet Security Alliance, a small business cyber security guidebook.
- Made available, for free, Cyber RiskProfiler™ with cyber scoring-technology developed and donated by nuServe℠ to assist small businesses in identifying and managing their cyber risks.
- Obtained cyber risk insurance premium credits from an insurance company. AIG eBusiness Risk Solutions, a division of the property-casualty insurance subsidiaries of American International Group, Inc. agreed in principle to provide credits, where legally permitted, on cyber-insurance policies for businesses that effectively implement task force awareness suggestions. The task force is looking forward to and seeks the participation of other qualified carriers in this program.
- Created an online small business cyber security resource center.

Home Users

Home User Awareness

The National Cyber Security Alliance (NCSA)—a non-profit public-private coalition of tech companies, owners and operators of critical infrastructures, and federal government agencies and departments— DHS and the Federal Trade Commission are recognized leaders in the home user awareness market. These organizations must continue to work closely together to implement a comprehensive awareness campaign.

Cyber Security Tips for Home Users

Contributed to updating and revising the NCSA's "Top 10" cyber security tips for home users.

Launch of Personal Firewall Day Web Site

Personal Firewall Day is dedicated to educating everyone about the threats we face—and pose— when we do not protect our computers with personal firewalls. Personal Firewall Day is also a call to firewall experts to share their expertise and advice with family, friends, and their communities.

Large Enterprises

General Business Community

The task force established relationships with trade associations representing the broad business community to explore ways to raise the level of cyber security awareness among C-suite executives.

Financial Services Community
The task force's efforts have been incorporated into the outreach efforts of the Finance and Banking Information Infrastructure Committee, headed by the Department of Treasury and the Financial Services Sector Coordinating Council. The council consists of 25 financial sector trade associations and holding cyber and physical security symposiums, hosted by the Federal Deposit Insurance Corporation, in 25 cities nationwide. These symposiums have reached in excess of 5,000 banking professionals and now include a session on how financial institutions can help home and small business users protect themselves from cyber attacks.

K-12 Education and Institutions of Higher Education
National Education Partnerships
CyberSmart! is a recognized leader in education and awareness to K-12 students. EDUCAUSE assists technology leaders at the nation's institutions of higher education in sharing information on best practices. The task force has built upon and leveraged the work of these two organizations to build relationships with this target audience.

Effective Security Practices Guide
The EDUCAUSE/Internet2 Computer and Network Security Task Force released the first-ever *Effective Security Practices Guide* for the higher education community, providing practical approaches to preventing, detecting, and responding to IT security problems in a wide range of higher education environments. The guide fulfills a recommendation from the *National Strategy to Secure Cyberspace* for colleges and universities "... to secure their cyber systems by establishing one or more sets of best practices for IT security."

State and Local Government
Created a pilot Web-based training tool for state and local governments, as well as businesses and home users, featuring a series of Webcasts.

Developed a concept for a national award recognizing achievement and leadership in cyber security by stats and local government information security professionals. The award would recognize teams, rather than individuals.

Enhanced Partnerships
Federal Trade Commission
The Awareness Task Force supports the FTC's "Dewie the Turtle" home user awareness campaign and "Operation Secure Your Server," an international effort headed by the Federal Trade Commission and 36 additional agencies in 26 countries to reduce the flow of unsolicited commercial e-mail by urging organizations to close "open relays" and "open proxies."

Open relays and open proxies are servers that allow any computer in the world to "bounce" or route e-mail through servers of other organizations, thereby disguising the real origin of the e-mail. Spammers often abuse these servers to flood the Internet with unwanted e-mail. Their abuses not only overload servers, but also could damage an unwitting business' reputation if it appears that the business sent the spam. "Operation Secure Your Server" provides businesses with simple, inexpensive ways to protect their computer systems from misuse.

Events

- Hosted a two-day workshop in conjunction with EDUCAUSE and CyberSmart! in January, focusing on outreach to K-12 and higher education students, executives, and staff.

- Conducted, in conjunction with the Internet Security Alliance, 10 focus group sessions, with almost 100 small business owners to provide content and feedback for the small business cyber security guidebook.

RECOMMENDATIONS AND NEXT STEPS

Small Businesses

- **Targeted, but Extensive Distribution of the Cyber Security Guidebook.** The U.S. Chamber of Commerce, the National Federation of Independent Businesses, the National Association of Manufacturers, and the Internet Security Alliance have each agreed to market the guidebook to its members and make it available on their Web sites. To distribute the guidebook to a larger audience, however, the task force has approached the Small Business Administration about the possibility of distributing the guidebook to small businesses. Initially, the guidebook will be an online resource. But to maximize the effect of this small business tool, the task force is looking for government and corporate sponsors to help underwrite the costs of producing and distributing large quantities of printed guidebooks.

Timeline: The preliminary text will be reviewed by the associations working on the campaign. Once organizations have signed off on the book's content (early April) the document will be typeset and electronically distributed. A printed version of the book is also planned for an April or May release, depending on funding levels required.

- **Increase Scope of Insurance Industry Participation:** The task force acknowledges the leadership of AIG eBusiness Risk Solutions, a division of the property-casualty insurance subsidiaries of American International Group, Inc., which agreed in principle to provide credits, where legally permitted, on cyber-insurance policies for businesses that effectively implement task force awareness suggestions. To gain broader support of this initiative, the task force will ask other insurance companies to provide financial incentives equivalent to AIG's discounts.

Timeline: This work will begin immediately, and the task force plans to announce partnerships with other insurance carriers by the fall.

Home Users

- **National Advertising Campaign:** The task force partnered with the National Cyber Security Alliance to update and revise its "Top 10" list of cyber security tips for home users. These tips will serve as the basis of a three-year national advertising campaign, which will be launched as soon as the financial resources are available.

Timeline: The launch of the national advertising campaign is tentatively scheduled for the fall.

- **Testing of initial advertising campaign.** This initial advertising campaign should be followed by a national opinion poll and then a follow-on campaign that takes into account strengths and weaknesses uncovered by poll findings.

Timeline: The testing of the initial advertising campaign will begin after the first year of the campaign's launch.

- **Leverage the access of Internet Service Providers (ISPs).** Since ISPs reach every home user of the Internet, the task force has partnered with the United States Internet Service Providers Association (USISPA) to determine how this access can be leveraged. In addition, colleges and universities serve as ISPs to nearly 20 million students and employees. The Task Force will continue to work with the ISPs to find creative ways to educate home users on cyber security issues.

Timeline: The USISPA and the National Cyber Security Alliance will meet in the spring to formalize a partnership.

- **Develop a Home User Cyber Security Tool Kit.** Create a cyber security kit for home users that provides detailed, easy to implement instructions on how to implement the "Top 10" tips list, CD tutorials with definitions, best practices and videos, vendor-neutral security checks, and mouse pads listing basic security tips. The tool kit could be distributed as part of the national awareness campaign by point-of-purchase retailers and by computer companies when sending their products to consumers.

Timeline: The tool kits are already in development and should be completed and ready for distribution by summer.

Large Enterprises

- **Create a CEO-Level Forum Series with DHS.** The task force believes that the best way to increase the level of cyber security awareness in large enterprises is to go directly to where the CEOs are. Therefore, we recommend that DHS join with leading business associations in hosting a series of regional homeland security forums. To add value, such forums need the direct support and participation of senior executives of DHS.

Timeline: In the spring, the task force will approach DHS to partner in this series. If DHS agrees, the task force will confirm the participation of various trade associations for this series. By summer, the task force, partner organizations, and DHS will announce a list of five pilot markets to test this program. The first regional CEO forum is expected in September.

- **Cyber Security Month.** The task force will create and promote an advertising program, primarily through print media, focusing CEOs of large enterprises on the issue of cyber security. The goal is to get free insertions of ads in publications that senior executives read.

Timeline: Since September is when most corporations focus on budgeting for the following year, the goal is to launch this campaign and the first regional CEO forum in September.

- **Direct mail campaign to the C-Suite executives of the 10,000 largest companies in America.** The purpose of the campaign is to provide senior corporate executives with key messages and activities that are necessary for enterprisewide cyber security.

Timeline: This direct mail campaign would be launched in July to precede September's Cyber Security Month and CEO forums and would be funded through corporate sponsors.

- **Provide seminars on cyber security best practices at major trade shows and perform Webinars.** These seminars and Webinars would target C-suite executives and be conducted by a paid consultant. The goal is to do one Webinar a month and have a presence at one trade show a month.

Timeline: Although intended as ongoing activities, the seminars and Webinars would begin in September, in conjunction with Cyber Security Awareness month.

- **Market and Distribute a Guide to Information Security for C-Suite Executives.** The task force will help distribute and raise awareness of the cyber risk management tools being developed by the Corporate Governance Task Force.

Timeline: The task force has received commitments from several business associations to help in distributing to their members the Corporate Governance Task Force recommendations. Further, the task force plans to distribute these tools at the proposed regional forums. A more extensive marketing campaign for these tools is expected by the summer.

K-12 Schools and Higher Education

- **Creation and Distribution of Awareness Material.** Often, direct communication and peer communication is the most effective means of influencing the behavior of this audience. Therefore, the task force will partner with CyberSmart! EDUCAUSE, Consortium for School Networking (CoSN) and others to create and distribute materials that raise awareness of appropriate cyber security behavior. Such materials might include posters, stickers, and brochures. The task force will seek to partner with school boards, teachers, state boards of education, the U.S. Department of Education, and institutions of higher education to explore how these entities can share these materials with their respective communities.

Timeline: The task force will finalize the awareness materials and formalize partnerships in the second quarter of 2004.

- **Provide Cyber Security and Ethics Curricula.** The task force believes that in addition to teaching students how to operate computers, schools should educate students on how to use the computer securely. The task force will develop curriculum material and explore opportunities for introducing awareness content as part of courses.

Timeline: Cyber Security curricula for K-12 students is expected in the fourth quarter of 2004.

- **Identify and Collect Effective Practices and Solutions.** By recognizing that the development of effective practices is a continuing process, the task force will continue to support higher education efforts to identify and catalogue effective practices for the *Effective Security Practices Guide*.

Timeline: Additional effective practices and solutions will be collected and disseminated during 2004, and a second version of the guide will be released in January 2005.

- By recognizing that the development of effective practices is a continuing process, the task force will continue to identify and catalogue effective practices for the Effective Security Practices Guide. The task force will disseminate the *Effective Security Practices Guide* to institutions of higher education.

Timeline: The task force has begun to catalogue existing best practices and will identify and disseminate them in the third quarter of 2004.

- **Create a DHS Regional Forum Series with University Presidents.** The task force will consider developing a homeland security forum series for university presidents, based on the DHS Homeland Security CEO Forums. A portion of the program should highlight the roles of university presidents in cyber security.

Timeline: After the launch of the CEO forum series in September, the task force will examine the value of replicating the series for university presidents.

State and Local Governments

- **Development of a Cyber Excellence Awards.** The State and Local Working Group developed a concept for a national award recognizing achievement and leadership in cyber security by state and local government information security professionals. The award would recognize teams rather than individual and could be based on a single act as well as a project. The task force recommends that the program be sponsored by DHS, with the winners being chosen by a committee of industry, academic, and government leaders. Next steps include approaching DHS about sponsoring the award and further refining award criteria and timing.

Timeline: In the spring, the task force will ask DHS to agree to sponsor the awards. If DHS agrees, the awards' criteria and timeline will be developed by the task force in conjunction with DHS by early summer.

- **Sharing and Promoting Effective Practices.** The task force inventoried existing best practice material for state and local governments, such as training employees on computer security, installing screen savers with cyber security tips, creating cyber security posters for the workplace, and contracting with vendors to enable home use as well as office use of their security products. From this inventory, the task force will select the most useful documents, update them as necessary, and publish them in a central location, such as a Web site.

Timeline: The task force expects to select the most beneficial best practice documents in the spring and begin dissemination to state and local governments in early summer.

- **Webcast Training.** The Task Force has agreed to develop a Web-based training tool for state and local governments. This tool will feature a series of Webcasts hosted by a variety of vendors, at no cost to the government, and will focus on a number of topics such as "security 101" and risk assessments. The tool will be posted on the Multi-State ISAC Web page, and the Multi-State ISAC will ask its members to push the tool to local governments. This feature will also be posted on the NCSA's site as a tool for home users and small businesses.

- **Timeline:** The first Webcast pilot has been finalized. This project is scheduled to be launched in mid April to a limited audience of approximately 200 people and available on the Web by the summer.

- **Support a State or a National Poster Contest for School Children.** The NCSA sponsors a national poster contest for school children. The task force recommends that each state support this effort by encouraging their students to participate. In addition, it recommends that each state promote cyber security practices by displaying the winning posters. In the absence of a national effort, each state is encouraged to develop its own statewide contest.

Timeline: The task force will coordinate the launch of the poster contest with the National Cyber Security Alliance. NCSA has not announced a timeline for its poster contest.

- **Measuring Success Survey.** The task force developed a one-page survey to obtain a baseline of where state and local government entities are in terms of cyber security awareness. The survey can be completed periodically to measure the success of the entity in promoting and developing cyber security awareness.

Timeline: The survey will be finalized and distributed to state and local governments by the end of spring.

- **Create a DHS Regional Forum Series with Governors.** The task force will consider developing a homeland security forum series for governors and mayors, based on the DHS Homeland Security CEO Forums. A portion of the program should highlight the roles of governors and mayors in cyber security.

Timeline: After the launch of the CEO forum series in September, the task force will examine the value of replicating the series for governors and mayors.

Report Appendix

The Awareness and Outreach Task Force
Working Group on K-12 Schools and Higher Education
Working Group Report

February 19, 2004

Background

The K-16 Working Group was assigned the task of developing an action agenda to reach K-12 schools and institutions of higher education with initiatives that will raise awareness and provide solutions regarding cyber security issues and practices. Our efforts comprise a part of the overall objective of the Awareness Task Force to institute and 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.

This reports presents an implementation strategy coupled with a tactical plan that targets K-12 students, parents, educators, and higher education. We focus on practical steps to increase awareness and manage the risks associated with the challenges of cyber security. This report does not contain resource requirements and estimated expenses associated with each action agenda item. However, following your review and as a next step we are happy to supply budget estimates.

The intent of this report is 1) to provide guidance to policy makers in the public and private sectors regarding the implementation of the *National Strategy to Secure Cyberspace* as it relates to outreach education, 2) to provide the private sector, non-profits, the education community and other stakeholders with direction and 3) to provide feedback to the Awareness Task Force Co-Chairs that will be efficiently coordinated with the input of other working group as a focal point for the conversation and actions associated with this critical issue.

The recommendations contained herein reflect the opinions of experts in K-16 cyber security education, and have been derived following years of experience in the field. The content for this report was substantially generated at the National Cyber Security Summit, December 3-4, 2003 and at the EDUCAUSE Security Education and Awareness Workshop, January 15-16, 2004.

The Problem

Stakeholders in K-12 and higher education have insufficient awareness and training with regard to cyber security issues and practices.

Consider the following:

- Just 30 percent of higher education institutions have implemented a cyber security education program (EDUCAUSE Center for Applied Research, 2003)

- An estimated 40 million young people in the U.S. spend significant amounts of time online. According to the National Cyber Security Alliance, many of them leave the family computer wide open to outside intrusion.

- Data from the Pew Research Center confirms that nearly all adults who download music from the Internet (including parents and college students) don't think they're stealing.

- According to the California Department of Education, only 13 percent of California's K-12 teachers consider themselves "proficient" at technology use.

Key Stakeholders

- Governing Boards for Institutions of Higher Education
- Higher Education faculty
- Higher Education staff
- Higher Education students
- Higher Education alumni and visitors
- Higher Education associations
- Senior K-12 administrators
- Boards of Education
- K-12 teachers
- K-12 curriculum developers
- K-12 students
- K-12 parents and other adult caregivers
- Education and hi-tech trade associations
- State departments of Education
- Hi-tech industry employers

Inventory of Work Areas

Common k-16 work areas

- Create and provide awareness-generating materials such as posters, stickers, certificates, etc.
- Develop curriculum materials and explore opportunities for introducing awareness content as part of course(s)
- Explore opportunities for introducing awareness as part of new employee of new student orientation.
- Media outreach intended to avoid cyber security paranoia while promoting interest in cyber security in an education context.
- Identify spokespersons for cyber security in education, which may include subject experts, well-known personalities, characters (such as Dewey the turtle).
- Engage trade associations in a coordinated effort to reach K-12 schools and higher education. Provide a template of content that associations can customize and distribute to their membership.
- Create and manage an online information sharing resource that will serve as both a focal point and repository of cyber security-related content, and a networking place for interested stakeholders.
- Incentive/Awards Programs
- Recognizing, with the possibility of "certifying" educators & students for achieving curricula goals, competency in the field of cyber security.
- Showcase exemplars (e.g., poster contests, innovative teaching methods, etc)
- Formative and summative assessment processes should provide quantifiable data regarding the impact of initiative, curricula, etc.

Work areas specific to K-12

Advocacy

Lobby state and federal lawmakers, departments of education and school districts to integrate cyber security and ethics curricula into state and nationally mandated standards. This should be done in an interdisciplinary manner (where cyber ethics, for example, would impact technology, social studies, science standards, among others).

Outreach

It's critical to emphasize continuing outreach, not just provide standards and instructional materials for the following stakeholders

- Teacher education: integrate cybersecurity/ethics curricula into state and national teaching certification requirements and ongoing professional development activities/requirements (e.g., Act 48 in PA)
- Parent awareness: cyber security in support of academic achievement and school policy
- School Board awareness: articulating the need for cyber security
- Provide cyber security and ethics curricula to K-12 schools
- Provide cyber security and ethics curricula to K-12 families
- Recommend IT staff training and certifications

Work areas specific to higher education
Resource Development

- Identify common problems and solutions to be converted into "messages" that will be common across user groups and organizational entities.
- Create and provide a model cyber security awareness programs for higher education. This will provide a template that the institution can customize to meet its individual needs. For example, a set of orientation materials that could be conveyed to first year students.
- Develop awareness content (e.g., web pages, posters, videos, etc.) that could be re-used by multiple institutions.
- Encourage collaboration and sharing of resources between academic programs (e.g., Centers for Academic Excellence in Information Assurance Education) and the operational needs to improve user awareness

Outreach

- Executive awareness: to include governing boards and senior administrators
- All users – baseline security awareness
- Information Assurance function – share best practices and models for team of individuals: IT security officer, risk manager, legal counsel, auditor, campus police or public safety, etc.
- Business functions – address security considerations that affect collection, maintenance, and use of sensitive or confidential data
- Provide awareness programs targeted to students: to include residential students and as part of orientation or academic programs
- Provide awareness programs targeted to faculty – both as "users" of technology and as "teachers" who can influence student behavior
- Provide awareness programs targeted to staff, especially consistent with their administrative function within the institution
- IT staff training and professional – identify and promote critical skills and competencies needed and identify or develop training programs

Continuity of Message
There should be a continuity of cyber security messages created by all Tasks Forces. For example, a set of cyber security tips adapted in an education program must not conflict with the messages communicated to home users, small businesses, enterprise employees, etc.

Action Agenda
The preliminary action agenda below includes projects already in place, along with new items to be developed and completed per the following schedule. The working group will leverage existing initiatives wherever possible (e.g., Consortium of School Networking (COSN), CyberSmart!, EDUCAUSE/Internet2 Computer and Network Security Task Force) with a concerted effort to involve stakeholders and players who provide value.

K-12 ACTIVITY	DELIVERY DATE	ASSIGNEE
K-middle school curriculum	Available/CyberSmart!	CyberSmart!
Identify and collect effective practices and solutions for training of IT staff	1Q2005	COSN/TBD

Provide IT staff training as needed	1Q2005	COSN/TBD
High school curriculum	3-4Q2004	CyberSmart! with Carnegie Mellon
Parent training	3-4Q2004	CyberSmart!
School administrator training	2Q2004	CyberSmart!
Teacher training	1-2Q2005	CyberSmart!
Outreach to K-12 schools via education associations, state departments and schools of education, large districts, etc.	Available/CyberSmart! (needs augmentation)	TBD
Targeted trade advertising to K-12 community	2Q2004	TBD
Creation/distribution of awareness generating materials such as posters, stickers, etc.	2Q2004 (some currently available)	CyberSmart!
Lobby to integrate cyber security/privacy/ethics into state-mandated teaching standards	2-3Q2004	TBD
Lobby to integrate cyber security, privacy, & ethics education into state and national teaching certification requirements	2-3Q2004	TBD
Awards/recognition program for best practices	3-4Q2004	CyberSmart!
Share best practices among educators	2Q2004	TBD
Certification/competency testing for curriculum/training completion at all levels: students, teachers, parents, administrators	3Q2004	TBD
Implement formalized assessment processes (metrics) for all curriculum and training programs which will yield measurable data regarding program impact (ie. curriculum)	2-3Q2004 for existing CyberSmart! Curriculum with others TBD	CyberSmart! and TBD
Establish a framework for determining training and certification needs		TBD

HIGHER EDUCATION ACTIVITY	**DELIVERY DATE**	**ASSIGNEE**
Conduct K-16 workshop to network, share effective practices and solutions and identify gaps in cyber security awareness education	1Q2004	EDUCAUSE
Collaborate with home user subcommittee of Awareness Task Force and National Cyber Security Alliance to identify common security messages	1Q2004	Security Task Force
Identify and collect effective practices and solutions among institutions	1-2Q2004	Security Task Force
Promote the observance of Cyber Security Day (April 4, 2004) by encouraging and supporting events around that date	2Q2004	Security Task Force
Draft model resolutions for discussion and use by academic senates or student government bodies	2Q2004	Security Task Force

Establish a Cyber Security newsletter for higher education	2Q2004	Security Task Force
Highlight effective practices and solutions during EDUCAUSE and Internet2 Security Professionals Workshop	2Q2004	Security Task Force
Sharing effective practices and solutions among institutions	2-3Q2004	Security Task Force
Establish a Speakers Bureau for cyber security awareness	2-3Q2004	Security Task Force
Develop and disseminate a Security Awareness Toolkit for colleges and universities	3Q2004	Security Task Force
Develop an awareness video for college and university executives	3Q2004	Security Task Force
Inventory practices and highlight effective practices and solutions for K-12 teacher education & awareness	3Q2004	Security Task Force & COSN
Establish a student contest for the development of an awareness video targeted to students that can be re-used by multiple institutions	3-4Q2004	Security Task Force
Identify and collect effective practices and solutions for training of IT staff	4Q2004	Security Task Force
Create model cyber security awareness curriculum	4Q2004	Security Task Force
Conduct a pre-conference seminar on how to conduct security education and awareness at EDUCAUSE2004	4Q2004	Security Task Force
Promote the observance of Cyber Security Day (October 31, 2004) by encouraging and supporting events around that date	4Q2004	Security Task Force
Establish an easy-to-replicate tool and database of questions for the establishment of an online quiz	1Q2005	Security Task Force
Establish or adopt an online tutorial and self-assessment instrument for general user education	1Q2005	Security Task Force
Implement formalized assessment processes (metrics) for curriculum and awareness programs which will yield measurable data regarding program impact	1Q2005	Security Task Force
Awards/recognition programs for best practices	2-3Q2005	EDUCAUSE
Objective to double number of institutions with cyber security awareness programs in place	2Q3Q2005	Security Task Force

Working Group Members

Dena Haritos Tsamitis, Carnegie Mellon CyLab and Information Networking Institute
Jim Teicher, CyberSmart!
Rodney Petersen, Educause
Charles Livingston, National Defense University
Barbara Laswell, SEI/CERT

EDUCAUSE Workshop Participants

Raymond Albert, University of Maine at Fort Kent
Robin Anderson, University of Maryland, Baltimore County
Cedric Bennett, Stanford University
Kelley Bogart, University of Arizona
Mark Bruhn, Indiana University
Paige Buechley, Texas State Auditor's Office
Daniel Caprio, Federal Trade Commission
David Escalante, Boston College
Amy Ginther, University of Maryland
Melissa Guenter, Consultant
Tiffany Olson Jones, Symantec Corporation
Lance Jordan, Rutgers University
Richard Lesniak, University at Buffalo
Mark Luker, EDUCAUSE
Vic Macaonachy, National Security Agency
Peter Martino, U.S. Department of Homeland Security
Jeffrey McCabe, Texas A&M University
Steve Miller, Consortium on School Networking/Mass Networks Education Partnership
Shirley Payne, University of Virginia
Rodney Petersen, EDUCAUSE
Davina Pruitt-Mentle, University of Maryland
Corey Schou, Idaho State University
Chris Seiberling, Consortium on School Networking/Mass Networks Education Partnership
Jack Suess, University of Maryland, Baltimore County
Elizabeth Sweet, University of Michigan
Jim Teicher, CyberSmart
Dena Haritos Tsamitis, Carnegie Mellon University
Valerie Vogel, EDUCAUSE/Internet2
Calvin Weeks, University of Oklahoma

Select List of Cyber Security Awareness Activities

Industry

The American Institute of Certified Public Accountants
http://www.aicpa.org/pubs/jofa/jun2002/quinn.htm
This links to a paper that addresses the role of CPAs in information security. The American Institute of Certified Public Accountants is the national, professional organization for all Certified Public Accountants. Its mission is to provide members with the resources, information, and leadership that enable them to provide valuable services in the highest professional manner to benefit the public as well as employers and clients.

The Business Roundtable
http://www.brtable.org
The Business Roundtable's Digital Economy Task Force has produced a resource to help CEOs and their senior executives develop a robust, effective program to protect their business as they incorporate sophisticated information systems into their operations. The resource includes recommendations for furthering corporate cyber security programs; a depiction of the need for not just technology but also policy issues in a successful program; and a list of key government contacts and Internet sites with more information on cyber security. Access the resource at **http://www.brtable.org/document.cfm/814**.

The Business Software Alliance
http://www.bsa.org
The Business Software Alliance (BSA), with programs in 65 countries worldwide, is dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry before governments and in the international marketplace. BSA also educates consumers on software management and copyright protection, cyber security, trade, e-commerce and other Internet-related issues. Visit their security page: **http://www.bsa.org/usa/policy/security/issue/index.phtml**.

Center for Internet Security
http://www.cisecurity.org
CIS provides methods and tools to improve, measure, monitor, and compare the security status of Internet-connected systems and appliances.

The Information Technology Association of America
http://www.itaa.org/infosec
ITAA seeks to improve the information security of the nation's critical information infrastructure in both the private and public sectors. This site includes links to news articles, press releases and reports.

The Institute of Internal Auditors
http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=132
The IIA and its partners released *Information Security Management and Assurance: A Call to Action for Corporate Governance*. The report advises board members to pay attention to information security issues, stating the Internet introduces new risks to every

organization. It contains 10 questions board members should ask in assessing the state of information security within the organizations they govern.

The Internet Security Alliance
http://www.isalliance.org/
The Internet Security Alliance is a collaborative effort between Carnegie Mellon's CERT Coordination Center and the Electronic Industries Alliance to promote sound information security practices, policies, and technologies that enhance the security of the Internet and global information systems. The ISA recently released a guide to 10 of the highest priority and most frequently recommended security practices for business.

Government

Computer Crime and Intellectual Property Section, U.S. Department of Justice
http://www.usdoj.gov/criminal/cybercrime/index.html
The Computer Crime and Intellectual Property Section ("CCIPS") attorney staff focus exclusively on the issues raised by computer and intellectual property crime. Section attorneys advise federal prosecutors and law enforcement agents; comment upon and propose legislation; coordinate international efforts to combat computer crime; litigate cases; and train all law enforcement groups. This website includes lesson plans and information for kids on cyberethics at:
http://www.cybercrime.gov/rules/kidinternet.htm

The Federal Trade Commission
www.ftc.gov/infosecurity
The Federal Trade Commission has created this website for consumers and businesses as a source of information about computer security and safeguarding personal information.

National Institute of Standards and Technology Computer Security Resource Center's Small Business Corner
http://csrc.nist.gov/SBC
The mission of NIST's Computer Security Division is to improve information systems security. This site focuses on resources for small businesses.

The National Strategy to Secure Cyberspace
http://www.whitehouse.gov/pcipb/
The National Strategy to Secure Cyberspace, an implementing component of the National Strategy for Homeland Security, is part of the White House's overall effort to protect the Nation. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, or control, or with which they interact.

U.S. Department of Education Internet Safety Page
http://www.ed.gov/Technology/safety.html
The Education Department's Office of Educational Technology works to assist the education community with meeting the national goals for educational technology.

United States Postal Service
http://www.usps.com
The United States Postal Service offers a Web site with information about its comprehensive privacy framework. The site also provides links to other resources and tools dealing with a host of privacy issues. Visit their Privacy Office: **http://www.usps.com/privacyoffice/welcome.htm**.

The World Bank
http://www.worldbank.org
To educate policy makers, businesses, consumers of financial services, and others involved in E-finance and E-commerce, the World Bank offers an **E-security Site** focusing on the complex trade-offs and actions needed to manage the risks of fraud and of compromising the security of digital assets. The site includes links to the World Bank's conferences, including its September 2002 seminar, **Global Dialogue E-Security: Risk Mitigation in Financial Transactions**, and also serves as a clearinghouse for knowledge on managing the risks associated with open network architectures.

Non Profits and Partnerships

The Asia Oceania Electronic Marketplace Association
http://www.aoema.org
The Asia Oceania Electronic Marketplace Association (AOEMA) was formed to promote the use of electronic commerce in the Asian region. Working closely with Asia-Pacific Economic Cooperation, AOEMA has done a number of projects on the barriers to electronic commerce, including this booklet to help you protect yourself when using the internet: **http://www.aoema.org/safetynet.htm**.

BBBOnLine
http://www.bbbonline.org
BBBOnLine is the arm of the Council of Better Business Bureaus that specifically deals with web sites. Working in concert with the 142 local BBBs in the United States and Canada, BBBOnLine encourages sound and ethical online business practices through its Privacy program, Reliability program, BBB Code of Online Business Practices, and an international initiative to promote safe e-commerce.

CERT Coordination Center's Home Network Security Tips
http://www.cert.org/tech_tips/home_networks.html
The CERT Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. CERT's information ranges from protecting your system against potential problems to reacting to current problems to predicting future problems.

Consumerreports.org
http://www.consumerreports.org/static/0206com0.html
Consumer Reports' Cyberspace Invaders site includes practical advice for consumers and a link to CR's online subscriber security survey. It also includes consumer security product ratings.

The Cyber Citizen Partnership
http://cybercitizenship.org
The Cybercitizen Awareness Program educates children and young adults on the dangers and consequences of cyber crime. By reaching out to parents and teachers, the program is designed to establish a broad sense of responsibility and community in an effort to develop in young people smart, ethical, and socially conscious online behavior.

CyberSmart!
http://www.cybersmart.org
CyberSmart! provides a comprehensive set of free lesson plans, student activities, and related materials for teachers and families to introduce the skills associated with 21st Century literacy, citizenship, and ethics. These skills provide the building blocks in order for children to be safe, responsible, and effective 21st Century citizens and learners. To access the CyberSmart! Curriculum, **click here**.

GetNetWise -- About Security
http://security.getnetwise.org/
The GetNetWise.org security section was established to deliver information and materials to consumers to protect their information and networks from theft, misuse and destruction. The site includes tutorials on how to use common software programs to enhance security and privacy.

The National Center for Missing and Exploited Children's NetSmartz Workshop
http://www.netsmartz.org
The NetSmartz Workshop is an educational resource for children of all ages, parents and teachers on how to stay safer on the Internet. NetSmartz is a project of the National Center for Missing and Exploited Children and Compaq.

National Cyber Security Alliance
http://www.staysafeonline.info/
The National Cyber Security Alliance is a cooperative effort between industry and government organizations to foster awareness of cyber security through educational outreach and public awareness.

NetSafeKids
http://www.NetSafeKids.org
NetSafeKids is produced by the National Research Council of the National Academies. The site offers essential information and practical tips that will help parents and adults make more informed decisions about how children spend time online.

Organisation for Economic Co-Operation and Development
http://www.oecd.org/ict/guidelines
OECD governments have drawn up new Guidelines for the Security of Information Systems and Networks in the wake of last year's September 11 attacks in the United States, in order to counter cyberterrorism, computer viruses, hacking and other threats.

Top 10 Cyber Security Tips

1. Use "*anti-virus software*" and keep it up to date.
Make sure you have anti-virus software on your computer! Anti-virus software is designed to protect you and your computer against known viruses so you don't have to worry. But with new viruses emerging daily, anti-virus programs need regular updates, like annual flu shots, to recognize these new viruses. Be sure to update your anti-virus software regularly! The more often you keep it updated, say once a week, the better. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to get regular updates for your software. Stop viruses in their tracks!

2. Don't open email or attachments from unknown sources. Be suspicious of any unexpected email attachments even if it appears to be from someone you know.
A simple rule of thumb is that if you don't know the person who is sending you an email, be very careful about opening the email and any file attached to it. Should you receive a suspicious email, the best thing to do is to delete the entire message, including any attachment. . If you are determined to open a file from an unknown source, save it first and run your virus checker on that file, but also understand that there is still a risk. If the mail appears to be from someone you know, still treat it with caution if it has a suspicious subject line (e.g. "Iloveyou" or "Anna Kounikova") or if it ortherwise seems suspicious (e.g., it was sent in the middle of the night). Also be careful if you receive many copies of the same message from either known or unknown sources. Finally, remember that even friends and family may accidentally send you a virus or the e-mail may have been sent from their machines without their knowledge. Such was the case with the "I Love You" virus that spread to millions of people in 2001. When in doubt, delete! If you receive an email from a trusted vendor or organization, be careful of phishing, a high-tech scam used to deceive consumers into providing personal data, including credit card numbers, etc. For information about "phishing" go to the FTC document titiled "How Not to Get Hooked By a Phishing Scam", http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf. The best way to make sure you're dealing with a merchant you trust, and not a fraudster, is to initiate the contact yourself. Type the merchant's address into your Internet browser instead of clicking on a link in an e-mail.

3. Protect your computer from Internet intruders – use "*firewalls*".
Equip your computer with a firewall! Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your personal computer and hardware firewalls that protect a number of computers at the same time. They work by filtering out unauthorized or potentially dangerous types of data from the Internet, while still allowing other (good) data to reach your computer. Firewalls also ensure that unauthorized persons can't gain access to your computer while you're connected to the Internet. You can find firewall hardware and software at most computer stores and in some operating systems. Don't let intruders in!

4. Regularly download security updates and "patches" for operating systems and other software.
Most major software companies today release updates and patches to close newly discovered vulnerabilities in their software. Sometimes bugs are discovered in a program that may allow a criminal hacker to attack your computer. Before most of these attacks occur, the software companies or vendors create free patches for you that they post on their web sites. You need to be sure you download and install the patches! Check your software vendors' web sites regularly for new security patches or use the automated patching features that some companies offer. Ensure that you are getting patches from the correct patch update site. Many systems have been compromised this past year by installing patches obtained from bogus update sites or emails that appear to be from a vendor that provides links to those bogus sites. If you don't have the time to do the work yourself, download and install a utility program to do it for you. There are available software programs that can perform this task for you. Stay informed!

5. Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long.
Passwords will only keep outsiders out if they are difficult to guess! Don't share your password, and don't use the same password in more than one place. If someone should happen to guess one of your passwords, you don't want them to be able to use it in other places. The golden rules of passwords are: (1) A password should have a minimum of 8 characters, be as meaningless as possible, and use uppercase letters, lowercase letters, symbols and numbers, e.g., xk2&LP97. (2) Change passwords regularly, at least every 90 days. (3) Do not give out your password to anyone! For enhanced security, use some form of two-factor authentication. Two-factor authentication is a way to gain access by combining something you know (PIN) with something you have (token or smart card).

6. Back up your computer data.
Experienced computer users know that there are two types of people: those who have already lost data and those who are going to experience the pain of losing data in the future. Back up small amounts of data on floppy disks and larger amounts on CDs. If you have access to a network, save copies of your data on another computer in the network. Many people make weekly backups of all their important data. And make sure you have your original software start-up disks handy and available in the event your computer system files get damaged. Be prepared!

7. Don't share access to your computers with strangers. Learn about file sharing risks.
Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to "share files". This ability to share files can be used to infect your computer with a virus or look at the files on your computer if you don't pay close attention. So, unless you really need this ability, make sure you turn off file-sharing. Check your operating system and your other program help files to learn how to disable file sharing. Don't share access to your computer with strangers!

8. Disconnect from the Internet when not in use.
Remember that the Digital Highway is a two-way road. You send and receive information on it. Disconnecting your computer from the Internet when you're not online lessens the chance that someone will be able to access your computer. And if you haven't kept your anti-virus software up-to-date, or don't have a firewall in place, someone could infect your computer or use it to harm someone else on the Internet. and help protect others: disconnect!

9. Check your security on a regular basis. When you change your clocks for daylight-savings time, reevaluate your computer security.
The programs and operating system on your computer have many valuable features that make your life easier, but can also leave you vulnerable to hackers and viruses. You should evaluate your computer security at least twice a year – do it when you change the clocks for daylight-savings! Look at the settings on applications that you have on your computer. Your browser software, for example, typically has a security setting in its preferences area. Check what settings you have and make sure you have the security level appropriate for you. Set a high bar for yourself!

10. Make sure your family members and/or your employees know what to do if your computer becomes infected.
It's important that everyone who uses a computer be aware of proper security practices. People should know how to update virus protection software, how to download security patches from software vendors and how to create a proper password. Make sure they know these tips too!

Awareness and Outreach Task Force
Membership List

Name	Organization
Scott Algeier	U. S Chamber of Commerce
Michael Allred	State of Utah
Blake Bishop	State of Florida
Dan Caprio	Federal Trade Commission
Lara Chamberlain	NFIB
Larry Clinton	Internet Security Alliance
Charles Curran	United States Internet Service Providers Association
Tom Dailey	United States Internet Service Providers Association
Chris Dixon	NASCIO
Sue Giatras	State of Utah
Bill Guidera,	Microsoft Corporation
Michael Gusky	State of Louisiana
Kai Tamara Hare	nuServe
James Holt	Saber Security Solutions
Andrew Howell	U.S. Chamber of Commerce
Jay Hoyer	Walnut Creek Chamber of Commerce
Tracy Hulver	TruSecure
Doug Johnson	American Bankers Association
Marc Jones	Visionael Corp.
Tiffany Jones	Symantec Corporation
Tom Kellermann	The World Bank
Irene Kinoshita,	Tysak
Jeff Klaben	Applied Materials
Charlie Le Grand	The Institute of Internal Auditors, Inc.
Charles Livingston	National Defense University
Dan Lohrmann	State of Michigan
Louis Malafarina	Public Intelligence
Dan McCall	Guardent
Stuart McKee	State of Washington
Time McNulty	AirZip
Steven Miller	Mass Networks Education Partnership
Mell Mireles	State of Texas, Department of Information Resource
Krista Montie	State of New York, CSCIC
Margaret Morrissey	State of New York, CSCIC
Wil Pelgrin	State of New York, CSCIC
Rodney Petersen	EDUCAUSE
David Peyton	National Association of Manufacturers
Lynne Pizzini,	State of Montana
Debra Reiger,	State of California
Joe Richardson	U.S. Department of State
Larry Rogers	Software Engineering Institute

Awareness and Outreach Task Force
Membership List (cont)

Name	Organization
Mike Russo	State of Florida
Ty Sagalow	American International Group
Howard Schmidt	e-Bay
Chris Seiberling	Mass Networks Education Partnership
Arnie Shimo	Lockheed Martin Information Technology
Patty Strickland	Patty, State of Florida
Jim Teicher	CyberSmart!
Dena Tsamitis	Carnegie Mellon CyLab & INI
Ken Watson	Cisco Systems, Inc.
Donald Wilborn	Donald, U.S. Secret Service
Vic Winkler	Sun Microsystems
Todd Wittbold	The MITRE Corporation