



COMPUTER AND NETWORK
SECURITY
TASK FORCE

**Statement of John (Jack) Suess, CIO, UMBC, and Cochair of the
EDUCAUSE/Internet2 Computer and Network Security Task Force**

**National Cyber Security Awareness Month
Kick-Off Event**

**September 30, 2004
National Press Club
Washington, D.C.**

On behalf of colleges and universities across the United States, I am pleased to appear today in support of National Cyber Security Awareness Month. The higher education sector plays an important role in the cyber security of America. Through its core mission of teaching and learning, it is the main source of our future leaders, innovators, and technical workforce. Through research, it is the basic source of much of our new knowledge and subsequent technologies. As complex institutions, colleges and universities operate some of the world's largest collections of computers and high-speed networks.

I am the chief information officer of the University of Maryland, Baltimore County (UMBC). UMBC is a midsize institution devoted to research and undergraduate education with its own unique set of cyber security challenges. As CIO, I must constantly work to build a safe and secure networked computing environment through the combined approaches of establishing a secure technical architecture, developing and enforcing appropriate policies and procedures, and delivering education and awareness programs that communicate clear and effective messages to our students, faculty, and staff.

I am also the cochair of the EDUCAUSE/Internet2 Computer and Network Security Task Force. Established in July 2000, the task force is a national effort that is working to improve awareness among the EDUCAUSE and Internet2 memberships and throughout higher education. The task force actively promotes effective practices and solutions for the protection of information assets and critical infrastructures.

The task force coordinates its efforts on behalf of institutions of higher education and with the support of the Higher Education Information Technology Alliance, whose members include the American Council on Education, Association of American Universities, National Association of State Universities and Land-Grant Colleges, American Association of State Colleges and Universities, National Association of Independent Colleges and Universities, and the American Association of Community Colleges. These organizations, along with EDUCAUSE, Internet2, and the National Association of College and University Business Officers, join me today in the endorsement of National Cyber Security Awareness Month.

The task force prepared the *Higher Education Contribution to the National Strategy to Secure Cyberspace*. Among other recommendations, the *National Strategy* encourages colleges and universities to secure their cyber systems by establishing “one or more sets of best practices for IT security . . . [and] model user awareness programs and materials.” I am pleased to report today on progress in response to these challenges:

- In January of 2004, we issued an *Effective Security Practices Guide* to share practical approaches to preventing, detecting, and responding to IT security problems in a wide range of higher education environments. Designed with colleges and universities in mind, the guide balances the need for security with an open, collaborative networking environment. It includes information regarding the need for security awareness programs and examples of effective practices and solutions in the college and university setting.
- In April of 2005, we will hold the Third Annual Security Professionals Conference that will bring together IT security officers and practitioners from across the higher education landscape. This annual event is an opportunity to bring our community together to highlight technical solutions, security policies and procedures, and management issues, including successful approaches to security training and awareness.
- We have also established an education and awareness working group of the task force to increase the awareness of the associated risks of computer and network use and the corresponding responsibilities of higher education executives and end users of technology, including faculty, staff, and students. Accordingly, I would like to end by describing some of our initiatives that will correspond with National Cyber Security Awareness Month.

On October 6, EDUCAUSE will hold a national Webcast event, “Campus and National Approaches to Improving Cyber Security Awareness.” This program will describe the efforts of the National Cyber Security Alliance and will outline strategies and tools for security awareness in the college and university setting.

On October 11 and 12, the Virginia Alliance for Secure Computing and Networking will host a regional event, “Meeting IT Challenges: National Strategies and Local Solutions,” at the University of Virginia in Charlottesville. The president of James Madison University will kick off the event by describing the urgent need to educate computer users on security and to address this need as a cultural issue.

On October 12 and 13, Carnegie Mellon University’s CyLab will hold a symposium on cyber security policy and cyber security journalist awards ceremony here at the National Press Club in Washington, D.C. The symposium will focus on security awareness, including a panel with representatives from the National Cyber Security Alliance and the EDUCAUSE/Internet2 Security Task Force. The cyber security journalist awards recognize excellence in the journalistic coverage of cyber security issues which in turn leads to greater awareness.

Finally, October 18–22 is the week that the National Cyber Security Alliance has elected to focus on academic audiences. Accordingly, we have several initiatives planned during that week as part of the EDUCAUSE Annual Conference that will be held October 19–22 in Denver, Colorado. Every attendee at the conference (5,000 individuals from across higher education) will receive a CD that contains cyber security awareness resources, including sample posters, brochures, postcards, presentations, and other materials that colleges and universities have developed to increase awareness. I want to acknowledge and thank the National Cyber Security Alliance for its financial support of this effort. We will also hold a half-day seminar as a guide to implementing an effective security education and awareness program in college and university environments. This session will offer help in implementing a security awareness program by sharing best practices and providing tools. Several other announcements and events during the week will reinforce the importance of cyber security awareness as part of an overall information security program.

In closing, I want to observe that the complex, diverse computing environments in colleges and universities result in blended environments that are faced with many of the same issues confronted by businesses (large and small), Internet service providers (many of the computers connected to campus networks are personally owned), and home users (many students and employees who commute bring their home computers to campus). Therefore, we are happy to join in partnership with the National Cyber Security Alliance and others dedicated to promoting cyber security awareness in an effort to develop consistent and effective messages that will lead to the establishment of a culture of security in our homes, workplaces, schools, and academia.

For more information, contact:

Rodney Petersen
Security Task Force Coordinator
EDUCAUSE
(202)331-5368
rpetersen@educause.edu

Jack Suess
CIO
UMBC
(410)455-2582
jack@umbc.edu

More information about the EDUCAUSE/Internet2 Computer and Network Security Task Force is available at www.educause.edu/security