



TELECOMMUNICATIONS REPORT

October 1, 2004 Volume 70, Number 19

Reprinted with permission.

Subscriptions to Telecommunications Report are available by calling 800-638-8437.

ATIS, NSTAC TACKLE CONVERGENCE, NETWORK SECURITY ISSUES

With the convergence of the public-switched telephone network (PSTN) and Internet protocol (IP) networks into a global next-generation network, meeting network security and emergency preparedness communications needs becomes evermore challenging, said Phil Reitingger, senior security strategist for Microsoft Corp. and chairman of the National Security Telecommunications Advisory Committee's (NSTAC's) next-generation networks (NGN) task force.

While speaking today at a network security symposium and workshop sponsored by the Alliance for Telecommunications Industry Solutions (ATIS), Mr. Reitingger said, "In the post 9/11 environment . . . it's essential that we do our jobs as members of government, as members of the private sector to address convergence, national security, and emergency preparedness issues going forward."

The ATIS workshop, which runs through tomorrow and is being held at Intelsat's headquarters in Washington, is part of the organization's implementation phase of a security issues work plan finalized this past June by its Technology and Operations (TOPS) Council. Susan M. Miller, president and chief executive officer of ATIS, provided opening remarks this morning and outlined the purpose of the two-day event, which is to facilitate cooperation among industry experts in identifying solutions for telecom security concerns. David Barron, assistant vice president at BellSouth Corp. and chairman of NSTAC's industry executive subcommittee, gave the keynote address on security management.

NSTAC, which was established in 1982, is a Presidential advisory committee that provides recommendations on national security issues. Mr. Reitingger said it was critical that NSTAC work with other groups, such as ATIS, in addressing security needs, as NSTAC provides such groups with a channel to the executive branch. "NSTAC can provide a mechanism to take some of the work you're doing, crystalize it in Presidential recommendations" and take it directly to the Administration, he said.

Mr. Reitingger said the NGN Task Force is on a tight schedule and is hoping to get its work done by the next NSTAC meeting, which is in May 2005. Since holding its first meeting in August, the task force has identified several key issues to address, including cybersecurity, priority treatment of quality of service, identity management and authorization, changing roles of government and industry players, and criticality.

"Networks are partially converged already, which is why we're moving rapidly" to get the job done and address the needs of stakeholders, he said. Mr. Reitingger said one of the task force's working groups hopes to release within the next month a report on what can be done to address security needs now using existing technology. - Margaret Boles, mboles@tr.com