***Insurance Times*:** Bush cyber security expert warns of vulnerability

October 29, 2002, Vol. XXI No. 22

BOSTON (AP) — President Bush's top cyber security expert said the country's computer systems could be attacked at any time by anybody, and the federal government must quickly address those vulnerabilities.

Richard Clarke was in Boston last week to host a town hall meeting at the Massachusetts Institute of Technology on the administration's proposal to safeguard the country's computer systems.

The “National Strategy to Secure Cyberspace," released last month, makes nearly 60 suggestions for improving computer security for everyone from home users to corporations and government agencies.

“We don't know when (an attack could come), we don't know who, so we're focusing on how," Clarke said.

Clarke said terrorists are not the only threat to the country's computer network, but they are definitely high on the on the list of concerns.

“There's some evidence that al-Qaida has been trying to learn how to do this, that they've acquired cyber hacking tools, that they've used the Internet for reconnaissance, both physical reconnaissance and cyber reconnaissance," he said.

The Bush plan has been criticized for recommending, rather than mandating, safety precautions.

Its recommendations range from urging users to set tougher passwords to establishing industry centers where companies can share and resolve their vulnerabilities anonymously.

The report, which is open to public comment until Nov. 18, encourages software engineers to be more careful with products they design, and companies to test their internal cyber security regularly.

It also recommends a code of conduct for Internet providers to follow when an attack is underway.

One proposal, which was excised from the report in the final stages of drafting, would have required companies to pay money into a fund to improve national computer security.

Clarke said people are generally unaware of the damage a cyber attack could do.

“It's someone stealing your money, stealing your identity, downloading your files, potentially turning out the lights, potentially blowing up transformers or pipelines, confusing 911 systems, turning traffic lights off," he said.

“They may not result in death, but they'll do damage to the economy and potentially they'll damage national security," Clarke said.

Since the report was released in mid-September, Clarke said, public comment has focused on the need for the federal government to finance more research and development for new security technology, and to provide more assistance to cash-strapped state and local governments.

The public is also encouraging the government to use its procurement power to compel better security on computer systems.