

## **Security Conference Focuses on Collaboration**

*By Tim McElligott*

*Jan 10, 2006*

ORLANDO -- All oars went into the water this week at the inaugural Homeland Security for Networked Industries conference in Orlando, Fla., as representatives from the government, communications, transportation and utility sectors came together to discuss the need for collaboratively securing the nation's infrastructure.

Keynote speakers from the U.S. Department of the Interior, AT&T, The National Cyber Security Division of the Department of Homeland Security, Waste Management and McAfee launched the new conference by sharing their horror stories, success stories, reality checks and observations on what is needed to improve our ability to respond to disaster, terror and other threats to the networks and assets of our most vital industries.

"This is about securing our nation's infrastructure for a better prepared America," said W. Hord Tipton, chief information officer at the DOI.

Tipton urged greater collaboration between industries and used his department's recent yet ongoing transformation as an example of the challenges in improving communication between disparate groups. The DOI's 70,000 employees and 200,000 volunteers manage groups such as the U.S. Geological Survey, National Park Service, Bureau of Land Management, the Bureau of Indian Affairs and more.

Tipton and the other speakers agreed that not every contingency can be planned for, nor every threat mitigated. Therefore, a necessary first step for all industries is an honest assessment of risk.

"All assets are not created equal, so you have to be able to pick the ones that matter," said Eric Winsborrow, vice president of marketing at McAfee.

Despite working for a provider of security solutions, Winsborrow advised networked companies to complete a thorough risk management assessment before implementing security solutions. He said companies need to identify, assess and reduce risk by looking at their policies, the importance of various assets, the vulnerability of those assets and the existence of threats to them before deciding where and how to implement solutions.

He also said that risk assessment is a moving target as threats escalate in their intensity and in their intended targets.

This is one of the reasons AT&T Vice President of Operations Roberta Bienfait said, "You can't survive with a reactive approach."

She called for a more proactive, predictive and preventative approach to security threats as she warmed the audience by telling them that she typically avoids these conferences like the plague.

This type of approach leads to a better state of preparedness, which is essential for these critical industries. Bienfait said AT&T plans for potential outages every day and is even making contingency plans for a possible bird flu outbreak.

"[Such an event] could take 40% of our workforce. So we have to know how we would run our network without our employees," Bienfait said. "We need to build in that resiliency to survive. We need an un-tethered operational team that can operate from anywhere."

She also spoke of the realities of improving preparedness when it comes to the financial implications. "It's hard to convince business leaders to invest in something they can't see or they think will never happen," Bienfait said.

She urged security folks to not let others shoot holes in their continuity plans and proposed a focus on network-based security solutions that would withstand the 500,000 viruses a year we will see by the year 2010.

As for the industries working together to form a secure infrastructure, this conference was more of a stage-setting event for future collaboration.

"In 2006, we see a heightened collaboration between the public and private sector. Information sharing is critical, but it has to move beyond that to real collaboration to mitigate risks within and between these sectors," said Donald Purdy, acting director of the National Cyber Security Division of the Department of Homeland Security.

Purdy said that cyber space and the physical space are becoming increasingly interconnected and that both should be addressed simultaneously. He also said that people should not take comfort in thinking that attackers would not want to bring down the Internet because they depend on it so much. "That only goes so far," Purdy said.

There already is some progress being made on cross-industry collaboration. Various groups including Homeland Security will conduct a national cyber exercise next month called Cyber Storm to evaluate vulnerabilities to the infrastructure. Other groups and initiatives are underway such as the Sector Coordinating Council, the National Infrastructure Protection Plan, which has subsets including the International Disruption Working Group, the Control System Security Program and the Software Assessment Program, which aims to build a system using common standards for evaluating software vulnerabilities.

"If we don't raise the bar and articulate where we are going, we aren't going to get there together," Purdy said.

*Telephony* is the leading publication for all communications service providers: new and incumbent, wireline and wireless. We deliver insightful and thoughtful coverage of the news, technologies and business strategies driving the industry.