

## DHS to use more simulations in infrastructure protection

By Jill R. Aitoro 02/23/09

The Homeland Security Department will rely more on simulations to test the integrity of critical infrastructure and key resources, according to a 175-page plan released last week. But one security specialist said the plan was thin on details.

DHS will increase coordination with the science and technology community on requirements for the "development, maintenance and application of modeling capabilities," according to the [National Infrastructure Protection Plan](#) released on Feb. 19.

The plan -- an update of a 2006 strategy -- emphasized the need to incorporate simulations into training at agencies such as the Coast Guard, which is responsible for overseeing protection of the maritime transportation sector.

DHS will provide guidance on the testing of commercially available software tools, and look for opportunities for public-private partnerships, the plan stated. The principal modeling, simulation, and analysis organization is the National Infrastructure Simulation and Analysis Center, located at the Sandia and Los Alamos National laboratories in New Mexico and operated by the DHS Office of Infrastructure Protection.

Alan Paller, director of research at the SANS Institute, a nonprofit cybersecurity research group in Bethesda, Md., said the strategy is too broad.

"The authors [of the plan] are unable to communicate anything specific that these simulations do, have done, or will do," Paller said.

Furthermore, "[DHS] provides no proof that what they are doing matters, and they provide no plan of action -- just a laundry list of coordination activities," he said. "It's a shame the nation invested anything in this [document]."

Some observers [say](#) past simulation exercises such as DHS' 2006 and 2008 Cyber Storm drills did not go far enough to mirror an actual cyberattack, but few disagree that such drills are critical for revealing potential vulnerabilities.

"There's a huge need for more simulation and modeling in cybersecurity, particularly as it concerns control systems and their nexus to the physical security of critical infrastructures like the electric grid, water purification and chemical manufacturing," said Gregory Garcia, who served as assistant secretary of cybersecurity and telecommunications at DHS under the Bush administration and opened his own information security consulting firm, Garcia Strategies, last month.

He cited as a valuable lesson the 2007 Aurora experiment, in which researchers at Idaho National Laboratory

demonstrated they could hack into the programs that controlled a generator and manipulate settings so it would self-destruct. "Just a few thousand bytes of malicious code can tell a picture in a thousand words," he said.

---

**COMMENT ON THIS ARTICLE IN THE FORUM**

---

---

© 2009 BY NATIONAL JOURNAL GROUP, INC. ALL RIGHTS RESERVED