

## DHS' Cyber Storm III to test Obama's national cyber response plan

By [Jill R. Aitoro](#) 08/26/09

ATLANTA -- The Homeland Security Department's third large-scale cybersecurity drill in September 2010 will test the national cyber response plan currently being developed by the Obama administration, said industry and government participants in the simulation exercise during a conference on Tuesday.

Cyber Storm III will build upon the lessons learned in the two [previous exercises](#) that took place in February 2006 and March 2008, and provide the first opportunity to assess the [White House strategy](#) for responding to a cyberattack with nationwide impact.

"The national cyber response plan will be an offshoot of a lot of the findings that came out of Cyber Storm I and II that will formalize the roles and responsibilities," said Brett Lambo, director of the cyber exercises program in DHS' national cybersecurity division. He participated on an afternoon panel at the GFirst conference in Atlanta hosted by the department's U.S. Computer Emergency Readiness Team. "It's not a direct cause-and-effect relationship, but a lot of questions bubbled up [from the exercises]," followed by the announcement along with President Obama's 60-day cyber review that a response plan should be developed.

Details of the national cyber response plan are still being finalized through weekly meetings with stakeholders from federal government and industry. An initial report is scheduled to be released in November, less than a year before Cyber Storm III kicks off, said Robert Dix, vice president of government affairs and critical infrastructure protection at Juniper Networks, who is among the industry representatives involved in both the plan's development and the Cyber Storm exercises.

"Right now, there's arm-wresting happening -- identifying roles and responsibilities; determining what information needs to be shared, to whom and when," Dix said. "This is a fairly large group with varying levels of experience in different topical areas all making important contributions."

In the first Cyber Storm, DHS used simulated attacks to bring down parts of the Internet and test the abilities of different sectors to recover their networks. In the simulated Cyber Storm II, the Internet was used as an attack vector for spreading malicious software and other cyber threats through computer systems. DHS is now discussing with state and local government and industry what form Cyber Storm III will take.

DHS hopes Cyber Storm III will provide an opportunity to enhance methods for information sharing; better define roles and responsibilities, and bring all sectors with a stake in information security to the table to inform the effort.

"These are not technology issues; they're policy issues," Lambo said. "And these are the things we're going to try to enforce through Cyber Storm III."

Tests likely will target control systems that support the country's critical infrastructure, such as the electric grid

and transportation systems, Dix said. Homeland Security also will call upon subject matter specialists to develop the manufactured cyberattacks. "With all due respect, these are some of the creepy minds that are able to conjure up these scenarios that are real world likelihoods," Dix said.

While tests in the previous Cyber Storm exercises were customized to the participating markets, with various sectors defending their computer systems against different types of attacks, DHS plans to have participants in Cyber Storm III "fighting the same fight" against a common threat that might manifest itself differently across different organizations, Lambo said. He compared the strategy to the **Conficker worm**, which rapidly installed malicious software on computers running the Microsoft operating system and posed a contrasting threat for critical infrastructure organizations envisioning the shut-down of services versus federal agencies fearing the loss of sensitive information.

One objective of Cyber Storm III is to harmonize the various alert level systems used in government and the private sector so that all stakeholders at least speak the same language.

"Everyone has their own alert level system in states, private sectors and federal government, but we don't have each other's criteria," Lambo said. "If someone calls and says 'We just went to alert level red,' if I don't know what red is, that doesn't mean a damn thing to me... We're trying to tackle that monster."

Homeland Security has just begun planning Cyber Storm III and is focused on encouraging early participation from the state and local communities, and private sector, including the variety of infrastructure markets.

In the long term, Dix said, the true impact of the simulation on the administration's national response plan depends on follow-through.

"A lot of recommendations that came out of Cyber Storm I and II have not been touched or acted upon," he said. "If we're serious about improving our resiliency, we need to take this seriously. My hope is that with this administration's attention, we can raise the bar through action and not just reports that we place on a shelf."

---

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