EXHIBIT 31

Bloomberg BNA   Privacy & Security Law Report®

11 PVLR 404

Internet

White House Advisor Schmidt Discusses Online Trusted ID Plan, Fighting Botnets

By Joyce E. Cutler

SAN FRANCISCO—The private sector is going to be in the driver's seat for creating a framework for trusted identities in online transactions, White House Cybersecurity Coordinator Howard Schmidt said Feb. 29.

Schmidt, speaking at a session of the RSA Conference 2012, said that the core of the administration's National Strategy for Trusted Identities in Cyberspace (NSTIC) is to make sure individuals, businesses, and computer-to-computer activities can use interoperable digital credentials.

The cybersecurity chief stressed that the framework will draw on industry expertise and the marketplace to have online identities validated and privacy protections addressed.

"The government will be and is a consumer of this technology and not the one that is going to go out and build this. Government should not be in that business. It's not the core competency. It's not the role of the government, but clearly it's the idea of the marketplace being driven by innovators and entrepreneurs,'' Schmidt said.

In April 2011, the Obama White House released its final draft of the NSTIC, which it said is designed to make internet communications and transactions more secure to reduce fraud and identity theft (10 PVLR 618, 4/25/11).

The private sector will build it "so we can get out of this massive, expensive, password management environment that we live in today,'' Schmidt said.

> **BNA INSIGHTS ARCHIVE**
>
> Building an Online Identity Legal Framework: The Proposed National Strategy—Thomas J. Smedinghoff, Wildman Harrold, Chicago

Moving Against Botnets

The Commerce Department's National Institute of Standards and Technology and the Department of Homeland Security are teaming up with the private sector to look at a voluntary industry code of conduct to address detection and shutdown of botnets (10 PVLR 1377, 9/26/11).

Botnets are networks of infected computers used to launch malicious denial of service attacks, send spam, and store illegal content.

Australia through its internet association has an "iCode'' of conduct with its internet service providers to reduce these so-called "zombie" attacks, Schmidt noted. While Australia is still developing statistics about how effective the code is, "the bottom line is if we have 5 percent less botnets, that's better than where we are today,'' he said.

Industry has raised concerns that owners and operators would be opening themselves to more government regulation, Schmidt said.

"None of us can predict what somebody might think about in the future,'' he said. "But what we need to make sure is what we're doing right now is [that] we're doing what we can to reduce the likelihood [of a successful cyber-attack], so it doesn't give someone in the future ammunition to say [that the] 'private sector is not responding.'''

White House Cybersecurity Plan

In June 2011, Commerce release a final draft paper developing cybersecurity strategies for non-covered critical infrastructure (10 PVLR 871, 6/13/11), Ari Schwartz, NIST senior internet policy adviser said.

He added that "no one right now is suggesting regulating, but yet there's an acknowledgment there are security issues at hand."

Within the next 90 days, the government is going to ask its private sector partners to roll out the framework addressing the issue and "develop the group that will lead this thing going forward," Schmidt said.

"This is not something we're going to continue to sit by and watch. We know it's out there. We've admired the problem long enough. It's time to act on it. We have the right people, the right stakeholders, the right leaders on the government side to help facilitate it, and I think it's going to move forward in a rapid manner," Schmidt predicted.

For More Information

Further information on the RSA Conference 2012 is available at http://365.rsaconference.com/index.jspa.