

From: Taillon, Jeff

To: Godfrey, Rob <RobGodfrey@gov.sc.gov>  
Stirling, Bryan <BryanStirling@gov.sc.gov>  
Taillon, Jeff <JeffTaillon@gov.sc.gov>

Date: 11/21/2012 10:27:40 AM

Subject: Post and Courier: Haley explains what led to cyberattack; Revenue director resigns

---

**Post and Courier:** Haley explains what led to cyberattack; Revenue director resigns

<http://www.postandcourier.com/article/20121120/PC16/121129950/1006/haley-explains-what-led-to-cyberattack-revenue-director-resigns>

By Glenn Smith

Older computers, unencrypted Social Security numbers and a lack of stringent security protocols for signing into the system created “a cocktail for an attack” by cyber-hackers who breached state tax records, Gov. Nikki Haley said today.

Haley made the statement as she released the final report by Mandiant, the security firm hired by the state to determine the source and extent of the recent hack that put the financial information of millions at risk.

“Could we have done a better job?” Haley said. “Absolutely.”

But Haley said the true test will be the state’s response to the episode, and South Carolina intends to make itself as hacker-proof as possible in an age when such breaches are becoming more and more commonplace.

Haley also announced that the director of state Department of Revenue, James Etter, is resigning in the wake of the breach. His last day is Dec. 31, she said.

Haley said she still has confidence in Etter’s abilities, but “I think Jim and I both agree that we need a new set of eyes on the Department of Revenue.”

Haley said the breach affected 3.8 million individual taxpayers, 1.9 million dependents, 699,900 businesses, 3.3 million bank accounts and 5,000 credit card accounts, all of which are now expired.

The governor said Mandiant determined that the breach only impacted folks who filed their tax returns electronically with the state. “Anyone who filed by paper does not have to worry about the breach,” she said.

Mandiant officials have told The Post and Courier that the hacker targeted unsecured, third-party software on a state computer system. The attacker tricked a user into opening a malicious file that took advantage of that vulnerable software, authorities said.

Revenue’s login system for the computer also did not have the strongest protections available to verify users trying to get in, Mandiant said.

Haley said Mandiant also found 1970s-era equipment used by the state left it vulnerable.

Haley said the state was following Internal Revenue Service practices in keeping the Social Security numbers without encryption. That will change, the governor said, and she plans to notify the IRS that its rules need to change as well.

Haley said the state now knows exactly who has been compromised by the breach. Experian, the company hired by the state to provide a year’s worth of credit monitoring to taxpayers, will be notifying those who have signed up with the company. The state will be sending notification letters to those who have not registered with Experian, she said.

**Jeff Taillon**

(803) 734-5129|Direct Line

(803) 767-7653|Cell