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 10:28:58 AM
Subject: Greenville News: Haley pivots on data Safety

Greenville News: Haley pivots on data Safety
DOR chief out; governor says more should've been done
http://www.greenvilleonline.com/article/20121121/NEWS/311210024/Haley-pivots-data-Safety
By Tim Smith

COLUMBIA — Almost a month after telling South Carolina residents that the hacking of computers at the Department of Revenue couldn't be avoided, Gov. Nikki Haley now says there were problems with data protection at the agency and she has accepted the director's resignation.

Haley also said that the number of potential victims of the massive data breach has expanded and that each taxpayer compromised will be sent a letter by the Department of Revenue or an email by a credit-monitoring firm.

The governor said, however, that only electronic filers in the past decade need to be concerned. Those filing paper returns are safe, she said.

"We should have done more than we did," Haley said. "We should have done above and beyond what we did."

The 74.7 gigabytes of data that were stolen or potentially stolen include 3.8 million Social Security numbers, 3.3 million bank account numbers, data belonging to 699,900 businesses and 5,000 expired credit or debit cards, officials said.

The Social Security numbers of 1.9 million dependents of taxpayers also were exposed, Haley said.

The governor said that Mandiant, a private security firm that investigated the breach, found two major security vulnerabilities — a failure to use dual-verification in system access and a lack of encryption of Revenue Department data.

Haley said the agency didn't encrypt its data in storage other than credit cards because the Internal Revenue Service doesn't recommend encryption for Social Security numbers. She said she sent a letter to the IRS Tuesday suggesting that the agency require all states to encrypt their data.

The revenue departments for North Carolina and Georgia already encrypt all their data, GreenvilleOnline.com has reported.

Mandiant said the hacker appears to have gotten into the Revenue Department's system after sending an employee a malicious email in August. The employee, one of several sent the email, "clicked on the embedded link, unwittingly executed malware, and became compromised."

The malware likely stole the employee's user name and password, Mandiant said in its investigation report, allowing the hacker to navigate in the system and scout through its various systems.

On Aug. 29, Mandiant reported, the hacker used a program to obtain account passwords from six computer servers.

Eventually, the hacker compressed a mountain of data and sent it to a system on the Internet, Mandiant reported.

In all, the hacker compromised 44 systems at the Revenue Department, installed a "back-door" entry on one, and stole files or back-up data on three systems, Mandiant said, using 33 unique pieces of malicious software and programs.

The hacker's attacks were traced to four different IP addresses — the computer signatures that help authorities determine where attacks begin.

The Revenue Department had encrypted most of the 387,000 credit or debit cards and any data while it was being transmitted to or from the agency. The other data wasn't protected.

The hacking was discovered by the U.S. Secret Service, which notified the state on Oct. 10, officials have said. Haley publicly disclosed the breach on Oct. 26.

No arrests have been announced in the case.

Haley said the Revenue Department is now in the process of encrypting Social Security numbers.

James Etter, the agency's director, has resigned, Haley said. She said she has "the utmost respect for Etter and his wife."

"I think Jim and I came to an understanding that we need a new set of eyes on the Department of Revenue," she said. "I don't want this to be about Jim Etter because we were in compliance. The problem is you have an IRS situation that is not up to date."

Etter will stay on until Dec. 31, Haley said, and will be replaced by Bill Blume, executive director of the state's retirement system.

"This is a new era in time, where you can't work with 1970s equipment. You can't go with compliance standards of the federal government because both are outdated. What you have to do as governor is step forward, come up with your own plans for equipment, come up with your own plans for compliance and do everything that you can to protect the people of your state."

That, Haley said, has been the biggest lesson of the breach. She said she was "shocked" to learn that IRS didn't require encryption.

"Cyber attacks are going to happen," she said. "But what we can do is put so many layers in this process that it is awfully hard to get into."

She said every state "needs to be looking at this." She said South Carolinians filing in other states also need to be protected.

The state weeks ago set up a credit monitoring service for taxpayers and businesses. Haley said the credit-monitoring firm that deals mostly with individual taxpayers will notify those who have signed up for its service by email if it has been determined their data was part of the breach.

Though officials are looking at returns as far back as 1998, most of the exposed data came from returns filed since 2002, Haley said.

As of this week, she said, 843,604 taxpayers have signed up for credit monitoring.

She said officials are working on a plan for protecting every agency from similar cyber attacks.

"The Legislature and I can no longer allow us to have archaic data, archaic equipment and archaic systems that don't protect the most sensitive of information for the people of our state," she said. "So we're going to have to step up, all of us."

Jeff Taillon
(803) 734-5129|Direct Line

(803) 767-7653|Cell