From: Taillon, Jeff

To: Godfrey, Rob <RobGodfrey@gov.sc.gov>
Taillon, Jeff <JeffTaillon@gov.sc.gov>
Hall, Taylor <TaylorHall@gov.sc.gov>
churchl@email.sc.edu <churchl@email.sc.edu>
Stirling, Bryan <BryanStirling@gov.sc.gov>
Haltiwanger, Katherine <KatherineHaltiwanger@gov.sc.gov>
LeMoine, Leigh <LeighLeMoine@gov.sc.gov>
Walls, Courtney <CourtneyWalls@gov.sc.gov>
Soura, Christian <ChristianSoura@gov.sc.gov>
Pitts, Ted <TedPitts@gov.sc.gov>
Baker, Josh <JoshBaker@gov.sc.gov>
Bondurant, Kate <KateBondurant@gov.sc.gov>
Walker, Madison <MadisonWalker@gov.sc.gov>
Veldran, Katherine <KatherineVeldran@gov.sc.gov>
Patel, Swati <SwatiPatel@gov.sc.gov>
Schimsa, Rebecca <RebeccaSchimsa@gov.sc.gov>

Date: 11/15/2012 10:52:18 AM

Subject: Post and Courier: Haley orders new security measures following breach

---

Post and Courier: Haley orders new security measures following breach
http://www.postandcourier.com/article/20121115/PC16/121119530/1005/haley-orders-new-security-measures-following-breach
By Stephen Largen

COLUMBIA — Gov. Nikki Haley is requiring the 16 agencies under her control to implement new security measures after the massive cyberattack at one of the agencies.

Haley issued an executive order Wednesday that requires Cabinet agencies, including the breached S.C. Department of Revenue, to work with the Division of State Information Technology on security initiatives.

The Revenue Department wasn't using the free cybersecurity offered by DSIT for the servers that were breached in the attack.

That security will be beefed up with Haley's order. Several Cabinet agencies will split the cost of hiring four new full-time DSIT employees who will help provide 24-hour monitoring to look for unusual events or viruses on agency systems.

"We need somebody in the office 24 hours a day monitoring those computers to make sure that the second they see an intrusion, they can stop it," Haley said.

The move should take about 60 days to fully implement, Haley said.

The governor's order also will require the purchase of equipment that will immediately shut down an affected computer if it notices any files being improperly moved or viruses being downloaded.

Haley doesn't control the dozens of other agencies of state government outside her Cabinet, but she said the administration has encouraged them to add monitoring services.

As of Wednesday, no new agencies have added DSIT security following the breach, the division's leader

said.

Haley announced the security changes during a news conference.

About $160,300 in Homeland Security money from the State Law Enforcement Division will be used to purchase the new equipment from Mandiant, the company now conducting a review of how the breach occurred. A report on that review is expected this week, she said.

The new steps are designed to avoid a repeat of the recent cyberattack that compromised Social Security numbers for 3.8 million people who had paid state taxes since 1998, thousands of credit and debit card numbers, and information from as many as 657,000 S.C. businesses.

Haley said officials believe the hacker accessed servers through one computer work station. The new equipment, known as “The Hand,” would immediately shut down access to the system if such a breach was discovered, she said.

S.C. Inspector General Patrick Maley said every state agency has some form of protection in place to safeguard its computers. The problem is that this isn’t standardized, he said.

Although the agency didn’t use the DSIT monitoring, a Revenue Department spokeswoman said at the time of the breach that the agency had several other security features in place.

Those include monitoring from Trustwave, which officials have said was used instead of DSIT monitoring because Trustwave is compliant with credit card company standards for processing card information.

Mandiant is expected to address what exactly Trustwave was doing for the agency at the time of the breach. The company was charged with helping to protect credit card information, not the mass of tax return information compromised in the cyberattack.

Revenue Department spokeswoman Samantha Cheek said other security measures in place before the breach included two firewalls, regular virus scanning of all desktop and laptop computers, Web filtering and spam filtering.

None of those safeguards stopped the cyberattack.

Maley said the steps taken Wednesday are a short-term safety measure. His task is now to help come up with a long-term solution as part of an earlier Haley executive order, he said.

Jeff Taillon
(803) 734-5129|Direct Line
(803) 767-7653|Cell