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 10:50:07 AM

Subject: Patch: Hack Update: Gov. Haley Announces New Cyber-Security Measures

---

Patch: Hack Update: Gov. Haley Announces New Cyber-Security Measures
All cabinets to receive upgraded security.
http://northeastcolumbia.patch.com/articles/hack-update-gov-haley-announces-new-cyber-security-measures
By Shawn Drury

On Wednesday, in the latest in a series of media updates since it was revealed that the Department of Revenue's records had been hacked, Gov. Nikki Haley announced that a new measure has been taken to minimize the possibility of such attacks happening again.

Appearing with Budget and Control Board Executive Director Marcia Adams, Division of State Information Technology (DSIT) Director Jimmy Earley and State Inspector General Patrick Maley, Haley said that she had signed an executive order (see attached) that will direct all 16 Cabinet agencies to work with DSIT for the purpose of implementing network monitoring. The governor also said she hopes that the many non-Cabinet agencies will work with DSIT to improve network security.

The network monitoring device will be provided by Mandiant, the company that helped the Department of Revenue, after the hack. The device from Mandiant is known as The Hand. It provides 24/7 monitoring of networks and files. In the event of an intervention or an unusual event in a network, the device can freeze all data transactions.

The monitoring is meant to be comprehensive, and will have the capacity to identify the "downloading of viruses and malware, collect and monitor network traffic, intercede and interrupt in real time the download of detected viruses and malware to a specific network computer, and collect and correlate this information across all agencies so that they can better identify trends and common IT vulnerabilities" according to a release.

When a threat is identified, DSIT will notify the affected agency and ask that the infected computer or system be removed from the network.

Six DSIT personnel will track the state's networks.

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