

From: Taillon, Jeff

To: Godfrey, Rob <RobGodfrey@gov.sc.gov>

Taillon, Jeff <JeffTaillon@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>

Peters, Hal <HalPeters@gov.sc.gov>

Date: 11/16/2012 10:54:04 AM

Subject: WLTX: How the DMV Protects Your Data (Video)

WLTX: How the DMV Protects Your Data (Video)

<http://www.wltx.com/news/onyourside/article/209200/325/How-the-DMV-Protects-Your-Data>

By Nate Stewart

Columbia, SC (WLTX) -- On Wednesday, Governor Nikki Haley issued an executive order that calls for around the clock computer monitoring for all cabinet agencies.

News19 checked in with one of those agencies that has to protect some of the most sensitive data. The Department of Motor Vehicles data computers house drivers licenses, Social Security numbers, and even birth certificates. After the Department of Revenue data breach, News19 wanted to find out how the DMV protects that information.

J.R. Sanderson, Director of Operations with the DMV, says data security is so important at his agency, it's the agency's top priority. Sanderson tells us since the breach the DMV has gone back and looked at "almost every system, both from a hardware, software, and discipline perspective, to make sure we are protecting the citizens data."

The DMV says they see around 100 hacking attempts a month, mostly coming from China. To combat those they have a 24 hour network operations center and numerous network firewalls. Just like the Department of Revenue, the DMV also hires the security consultant Trustwave.

Through a Freedom of Information Act request, News19 obtained the contract between the DMV and Trustwave. According to it, they pay around \$20,000 annually for services that consists of penetration tests and vulnerability scans.

Sanderson says it would be a major fraud if someone were to penetrate the DMV network. "What you want as an agency is you want somebody on the outside attempting to brute force your firewalls or trying to see how disciplined you are by trying to hack in and get a password and user name and try to get into your system that way."

Sanderson tells News19 that twenty percent of the DMV's 80 million dollar budget is spent on purchasing software and hardware to protect tax payer data.

Jeff Taillon

(803) 734-5129|Direct Line

(803) 767-7653|Cell