

From: Pitts, Ted
To: Soura, Christian <ChristianSoura@gov.sc.gov>
Date: 11/12/2012 9:42:16 AM
Subject: FW: #2 OIG Update Letter re State-Wide INFOSEC Initiative
Attachments: update #2 letter (11112012) final.docx
Short Term Cyber Security Action Plan 11 05 12.docx

-----Original Message-----

From: Maley, Patrick
Sent: Sunday, November 11, 2012 3:34 PM
To: Pitts, Ted
Subject: #2 OIG Update Letter re State-Wide INFOSEC Initiative

Ted, attached is second update letter--hard copy signed letter to be mailed. Also attached is the email to all CIOs re short term cyber security procedures referenced in the letter. I am copy counting the Legislative leadership on the letter to keep everyone in the loop.

It is critical that the Governor fully understand how I have shaped my approach to address her executive order and her request for the OIG to conduct a "holistic" review of information security policy and procedures state-wide. This second update letter emphasizes the distinction that the OIG's role is fixing the organizational dysfunction issue, which is the core issue, rather than from a policy development and technical solutions perspective. These technical decisions on policies and unique mitigation strategies can only be executed by INFOSEC subject matter experts with that type of experience. The INFOSEC problem has been the state not building the organizational mechanism, a state-wide INFOSEC Program, with the right authorities, processes, and plan to systematically develop policy and technical solutions to understand & mitigate state-wide INFOSEC risk. Build the state-wide mechanism (the organizational issue), then it will be self-sustaining for the long haul and be able to adjust policy and technical solutions, among many other benefits, to meet changing threats & risks. We don't need a one time static fix of policies, procedures, and technology. Meeting with consultants last Friday reaffirmed this approach.

If her objectives or ideas differ, please let me know to see what we can factor the input into our overall approach.

My hope is for a governance & strategy interim report (milestone #1) be completed next week, or certainly the Monday after Thanksgiving. The recommendations bubbling up will be in the area of creating a Chief Information Security Officer (CISO), as well as a separate office. The CISO needs to report to a high official; there are several options. The CISO will need authority to set and enforce policy, either from existing legislation which has been under-exercised or new legislation. As the governance framework is built around the CISO, I am sure the CISO will need an advisory board from CIOs, as well as from other disciplines such as finance, procurement, legal etc. INFOSEC needs to be a governance issue for the entire state government operation, and not just an IT function.

INFOSEC strategy has 3 general options--maintain current decentralization, move up spectrum to a federated model, or go towards centralization. Really don't want to commit until I get all input from

CIOs because they understand the culture and have seen it all. However, other states all seem to be federated with a few being highly centralized. Experts and consultants work in the federated spectrum of a basic HQ authority for subject matter expertise & organizational mandatory policy umbrella, then agencies execute corporate policies by tailoring to their environment with final agency policies subject to HQ review, approval, and subsequent monitoring.

Will need to hire a consultant to help establish the governance framework (policy framework, structure/processes, communication plan, authority, prioritized statewide plan). Price 100-200k is just a guesstimate. Got to give thought of immediate Acting CISO so we have tangible state leadership leading the consultants, not the other way around, on the governance framework and start the relationship/trust with CIOs and other members of executive management.

As the governance model gets spun up, the OIG will work on implementation options with a contractor provided by BCB in terms of specific tasks, timeline, and costs for completion (milestone#2). I will certainly find group of CIOs to be in this endeavor to provide input. Rough, very rough, guesstimate is several million dollars. Implementation is boots on the ground consultants conducting risk assessments and developing mitigation strategies for individual agencies, often resulting in multi-year plans for each agency and estimated costs of mitigation. I believe there is also the capability to estimate costs for mitigation flowing from INFOSEC risk assessments based on experience consultants have from other state governments. These costs will be spread out of many fiscal years and I believe this is where the big dollars will be.

OK, after two weeks, that is where we are, and where we are going. I really need everyone to be clear on the OIG's role & responsibilities. There is time to recalibrate if there are differing objectives and ideas. I plan on sending out a press release Tuesday to open communication with the public on what we have done and where we are going, which will have data similar to this update #2 letter.

My cell is 803-429-4946. thanks