DOR Breach Senate Subcommittee
Meeting #6
January 22, 2013

REORGANIZATION OF THE *DEPARTMENT OF REVENUE'S* INFORMATION SECURITY PROGRAM

I. Testimony of Scott Shealy (Former DOR IT security administrator)

1. What was the organizational structure of the IT department and the information security office within the Department of Revenue during your tenure there?

2. Were there times when you agreed with Mr. Garon that certain security measures should not be implemented? If so, can you provide an example?

3. DOR has stated that after you left the employment at DOR, your job duties were delegated to remaining IT staff. In your opinion did the remaining staff have the qualifications and time (given their increased workloads) to handle these job duties?

4. DOR has stated that the devices acquired by DOR during your tenure there for encryption of data on hard drives, which was for laptops and desktops, proved to be cumbersome and ineffective. Would you agree with this assessment of the encryption on hand at DOR? Was the encryption technology available difficult to use consistently? Did you make recommendations to anyone at DOR concerning encryption? If so, what were your recommendations?

5. Did you have the ability to relay concerns regarding Mr. Garon, IT security, or your recommendations to DOR administration staff? Did you ever attempt to reach out to DOR administration staff?

6. Did you have the responsibility for ensuring DOR followed the mandates and recommendations of NASCIO, the IRS or PCI? In your opinion, were the minimum standards set by these regulatory entities not followed?

7. Did you ever relay concerns regarding a failure to comply with minimum standards or requirements or the need to implement additional measures above industry standards? If so, to whom?

8. Did you feel that you would be reprimanded if you took recommendations and concerns directly to the executive administration staff?

9. Did you report to Mr. Garon or to another intermediate supervisor who reported to Mr. Garon? Did you relay recommendations to Mr. Garon or your direct supervisor?

10. Were you aware of the agency's budget abilities/constraints? If so, did a lack of resources keep leadership, in your opinion, from implementing available best practice technologies (encryption at all levels, dual-factor authentication)?
11. Was senior DOR administration not made aware of or ignorant of best practices concerning security techniques? If so, why did they not know of the best practices? If not, are you suggesting that management knew of best practices concerning security techniques but decided that the risk of a loss/incident was small enough to warrant inaction?

12. Was a recommendation made to senior management to suspend monitoring at Market Pointe until all equipment was moved during DOR's relocation from Columbia Mills? If not, on what basis did management make this decision?

13. What are your recommendations for a successful organizational structure at DOR relative to IT and information security?

II. Testimony of Bill Blume (Newly-appointed Interim DOR Director)

1. Was the vendor for data encryption at DOR competitively bid following the standard procurement process?

2. Describe the process used to identify and evaluate the data encryption vendor?

3. How many proposals did DOR receive? Was the field of proposals narrowed to a few finalists? How many finalists were there and on what basis were they chosen or the others eliminated?

4. What are the qualifications of the individuals that made up the panel that selected the data encryption vendor?

5. Why was EMC selected over the other finalists?

6. Explain the differences between the level of encryption in place at DOR prior to the breach compared with the encryption services EMC will be providing. (data on hard drives vs. data at rest)

7. On what date was the contract with EMC signed?

8. What, if anything, does EMC need to do before they can begin encryption of the data at rest.

9. When is EMC expected to begin and complete the encryption of the data at rest?

10. How much is the contract with EMC?

11. Is cost for this encryption contract part of the $20.17 Million inter-agency loan DOR has received to address its IT infrastructure or is the cost in addition to the loan?

12. What other expenses has DOR incurred that is in addition to the $20.17 Million loan?

13. What organizational efforts have you made since you began work at DOR on January 2?

14. Does DOR have an information security officer (ISO) in place?

15. Does the ISO report directly to you (Bill Blume) as the executive director?

16. What plans are you working to implement over the next year?

17. What efforts are being made to manage a potential significant increase in paper tax returns due to the breach and the hesitancy of taxpayers to file electronically?