DOR Breach Senate Subcommittee
Meeting #1
November 28, 2012

DEPARTMENT OF REVENUE QUESTIONS

A. IT Security Decisions Over the Past Two Years

1. Describe the organizational structure of DOR's IT department and the size, expertise and background of its personnel at the time of the breach, to include areas of expertise, number of FTEs and temporary employees. Did the IT department at the time of the breach include cyber security experts? If not, has DOR now hired or have plans to hire a cyber security expert?

2. Prior to the breach, what procedures did DOR's IT department have in place concerning cyber security?

3. Prior to the breach, did DOR have any kind of proactive or reactive incident response plan to deal with situations like this hacking?

4. A prior executive order of the Governor required the Inspector General to work with agencies to determine what security measures are being used and to develop standard statewide security measures. What has the Inspector General reported concerning DOR's security measures in place before the breach?

5. Explain DOR's view and use of DSIT prior to the breach. Prior to the breach, was it DOR's opinion that DSIT services were: 1) not necessary 2) entirely duplicative of services DOR had contracted elsewhere for, 3) somewhat duplicative, 4) too expensive, 5) a combination of some or all of these? Please be specific.

6. During the past two years, have agency officials, whether IT or otherwise, attended conferences, seminars, workshops, and/or tradeshows focused on either IT generally, and/or cyber security specifically? If yes, when and who attended (by position if not name)? Was cyber security a topic and were cyber security general or breakout sessions attended by DOR employees? Was conference information shared with senior staff and were recommendations on enhanced cyber security protocols and/or services made? What was done with those recommendations?

7. To your knowledge, has the Internal Revenue Service (IRS) ever had a data breach and if so what was the magnitude?

8. Does the IRS have jurisdiction over DOR cyber security protocols?

9. At the time of the breach, did DOR utilize the exact same levels and types of cyber security protocols and protections as the IRS? If yes, what were they? If no, why not and what were the differences?

10. Does the IRS make specific state level recommendations for cyber security and, if so, please provide the subcommittee a copy of either the IRS's general recommendations and/or its specific recommendations for South Carolina.

11. Did the Director evaluate/undertake a needs assessment of the Department's "Information Technology" (IT) Division's cyber security capabilities upon nomination and/or appointment? If yes, approximately when did that initial evaluation occur, who was involved and what was the overall conclusion drawn from the initial evaluation?

12. Related to the initial assessment (if there was one), were specific cyber-security recommendations made by either DOR staff (including the Agency Director and/or the IT Director or either of their staffs) or outside experts (public or private)? If recommendations were made, please provide specifics as to who made the recommendations, what those recommendations were and whether or not they were implemented, and if yes, by whom and when?

13. Specifically, were the Agency's protocols, policies, and/or procedures regarding the "encryption" of data presented to, requested and/or discussed by the Agency Director or senior staff as part of any initial assessment that may have been undertaken regarding cyber security?

14. How regularly did senior staff, including the Agency Director, meet to discuss IT issues generally, and/or IT cyber security issues specifically? Please provide as specific a timeline as possible.

15. Prior to the breach being discovered, when was the last meeting of senior staff where cyber security was discussed generally (or specifically) and what was discussed?

16. Following the data breach at the Department of Health and Human Services, did senior DOR staff meet to discuss that agency's breach specifically, cyber-security generally, and/or the status of DOR's cyber-security protections and protocols? If yes, who met and when, and what conclusions or actions, if any, resulted?

17. Following the data breach at the Department of Motor Vehicles, did senior DOR staff meet to discuss that agency's breach specifically, cyber-security generally, and/or the status of DOR's cyber-security protections and protocols? If yes, who met and when, and what conclusions or actions, if any, resulted?

18. Related to the aforementioned data breaches at other state agencies, did senior DOR staff communicate with, or instruct staff to communicate with, or receive communications from: 1) other state agencies regarding IT security issues, 2) private vendors with whom DOR contracted with regarding IT security issues (i.e., Trustwave, etc), and/or 3) private vendors seeking to do business with DOR which offered cyber security protections? If yes, who communicated (or contacted) and when, and what actions, if any, resulted?

19. Did DOR staff/other state agency staff/contracted private vendor staff make specific requests and/or recommendations to senior staff regarding the agency's cyber security procedures and protections that were not acted upon? If yes, what were those recommendations and why were they not acted upon?

20. Please describe in detail your "internal" data security controls for both DOR employees and any contract staff in place before the breach occurred. Please indicate whether or not policies were in writing (and be prepared to provide copies) and the process by which employees were made aware of the policies, etc. Also note policies, if any, regarding internet access generally (who, if anyone, could "surf" the web and for what reasons) and related, email access, to include policies regarding accessing by employees of "personal" email accounts (i.e., Gmail, yahoo, AOL, etc). Also, did DOR utilize "internet monitoring" programs to monitor employees utilization of (and adherence to DOR policies) the internet and/or email accounts. If yes, how (and for what purposes) was the data used and how and when was such information reported to senior staff, if at all?

21. Related, pre-breach, did DOR have (and did it encourage, and if yes, how so?) a protocol by which employees (whether direct or contract) were supposed to notify Agency officials of any suspicious emails or internet activity and related, were employees "trained" or "educated" on what "suspicious" emails or internet activity may "look like"? Please be specific.

22. Was DOR receiving all the services from Trustwave it thought it was receiving under contract? Were there any services DOR had an expectation Trustwave was providing that it now knows the company actually was not providing?

23. How often was Trustwave providing intrusion detection and vulnerability scans? How does this compare with best practices concerning the frequency of such scans? How do such scans compare with the frequency of similar scans offered by DSIT?

24. Do any other agencies that accept credit card payments use Trustwave services?

25. Part of Trustwave's compliance validation service for payment card compliance is to identify any non-compliance issues based on an online self-assessment questionnaire. Has Trustwave ever identified any non-compliance issues? If so, how were those issues addressed by DOR?

26. DOR was recently quoted as saying that a reason DOR did not engage the services of DSIT was that some of its services would be "redundant" with DOR's contracted vendor Trustwave. Please cite specifically which services would have been redundant. Was the redundancy noted viewed as a negative?

27. What services, if any, did Trustwave provide that are specifically relevant to the DOR breach and did those services meet your needs and expectations regarding the breach? If yes, how so? If no, how so?

28. Prior to the breach, did you contract with Trustwave exclusively for, or primarily for, “PCI compliancy”? Please explain to the subcommittee what PCI compliancy is and indicate whether or not being PCI compliant had an real bearing on the specifics of this breach? Specifically, should being PCI compliant have been expected to either prevent or mitigate the magnitude of this breach?

B. IT Protections in Place at the Time of Breach

1. Reports state that the system was breached four times before the activity recognized and thereafter reported by the Secret Service? Why didn't DOR or Trustwave recognize the system was being breached until after the Secret Service notified the agency? Had the Secret Service not detected the breach, when would Trustwave or DOR have discovered the breach?

2. Does the current breach fall within the suspicious activities that are monitored under the "Network Penetration" and "Policy & Procedure" services provided by Trustwave under contract? If so, why did these protections fail to identify the breach at DOR?

3. One of the contracted services with Trustwave is to perform a probe of all systems in the network and identify all vectors that might be exploitable, which could allow Trustwave to devise an attack strategy and proceed with an attempt to exploit identified vectors. It is, however, up to DOR to decide whether to allow Trustwave to proceed with a controlled exploitation of the system. Has DOR allowed Trustwave in the past to proceed with a controlled exploitation of identified vectors?

4. How do the services offered by DSIT concerning cyber-hacking protection compare with the services to be provided by Trustwave under its contract with DOR?

5. From what sources has the State obtained its information in indicating that industry standard is not to encrypt and that most banks do not encrypt? What is the industry standard concerning cyber-hacking protections? How does industry standard compare with system security best practices?

6. Prior to the breach, when did DOR last look at encryption as a possibility and what was found to be the cost and time associated with that? What is the current cost to encrypt?

7. Was encryption ever actually considered by DOR? If so, was the decision of DOR not to encrypt driven by budget limitations rather than by industry standards or best practices? Has DOR ever asked for or considered asking for funding specifically for encryption of taxpayer data or other cyber security measures?

8. DSIT has indicated that it provided some monitoring at DOR's Columbia Mills location. To what extent was DSIT monitoring this location? Why wasn't DSIT asked to provide data monitoring services as part of DOR's ongoing relocation to Market Pointe?

9. DOR has indicated that the agency contracted with Trustwave for its Payment Card Industry (PCI) compliance services that DSIT does not offer. When was the last time another company was considered to provide these services? Were the contracts with Trustwave part of an RFP process? If not, why?

C. Efforts Made to Close Holes and Enforce IT Protections after Breach

1. Describe the contacts DOR had with Trustwave after breach.

2. Describe the contacts DOR had with DSIT after breach.

3. Explain the details of DOR's contractual relationship with Mandiant. What were they hired to do, when and for how long?

4. When was Mandiant first contacted? When was an agreement for software and services with Mandiant agreed upon.

5. As to the credit monitoring services being provided by Experian, when were Citreas and IdentityForce, as noted by DOR legal counsel, contacted regarding the credit monitoring services they offer?

6. What were the differences between the services and costs offered by Experian and the other two providers?

7. By what process were Mandiant's services procured? What the procurement of Mandiant's services done with guidance from the Procurement Office?

8. How does DOR plan to pay for additional costs that will result from the DOR breach? (increased paper tax returns, etc.)

9. It appears other software similar to the Mandiant Intelligent Response (MIR) appliance, or "The Hand", exists in the market. With multiple options available, was a procurement process followed in selecting Mandiant?

10. To what extent were other similar programs/appliances considered? Why was Mandiant chosen over other programs?

11. What measures has DOR taken and/or will continue to take to close the gap between when a breach is occurring and when it is identified?

12. How have DOR's IT policies and procedures concerning data security changed since the breach.

Which of the contracts DOR has entered into (Trustwave, Mandiant, Experian, Dun & Bradstreet) have been determined to be entered into as an emergency procurement? Can DOR provide the written justification to satisfy the audit requirements of SC Code 11-35-210?

13. Breach Response Plan: Prior to the breach, did DOR have in place a written "plan of action" of how DOR staff was to respond to the breach? If no, why not? Related, if no, has DOR developed, or is it in the process of developing, such a written plan? If yes, please provide a copy of the plan and describe how the plan was either followed or deviated from after this specific breach.

D. Notifications to and Protections for Taxpayers Concerning Breach

1. According to the Experian contract, DOR had to provide Experian with a list of individuals eligible to receive activation codes/services from Experian. Why then could DOR not contract with Experian to monitor all social security numbers provided instead of requiring each individual to call and enroll?

2. Did the State sign a contract with Dun & Bradstreet for the free services they are providing? If so, can a copy of the agreement be provided?

3. When will the Family Secure Consumer Product offered through Experian be available for families? When will the activation code for this product be delivered to individuals? Will the lapse in time between the time the breach occurred and the time the Family Secure product is made available create a greater likelihood of minors' data being used?

4. Are individuals that were already enrolled in Experian services prior to the breach eligible for the free Family Secure Product? If so, how will these individuals be notified?

5. How does DOR plan to pay for the $12 Million Experian contract?