DOR Breach Senate Subcommittee
Meeting #4
January 3, 2013

PREPARED QUESTIONS BY SUBCOMMITTEE POSED TO GOVERNOR'S OFFICE:

I. Negotiation and Details of Experian Contract

1. Have there been any discussions with Experian or another credit monitoring company regarding the continuation of monitoring services for taxpayers after the initial year?

2. The contract with Experian was labeled as an emergency procurement. By definition, emergency procurements are limited to those supplies, services, information technology or construction items necessary to meet the emergency. The emergency in the recent DOR breach was identifying the source and cause of the breach, closing any holes through which additional information could be stolen, and tracing the criminal or criminals who hacked into the system. Mandiant was hired as an emergency procurement to assist with this initial investigation and to make short term recommendations to secure the system against another immediate threat.

   Given that the nature of Experian's services is to provide information and reactive assistance after an identity theft or fraud has already occurred, please explain the reasoning behind classifying the Experian contract as an emergency procurement.

3. Did the Governor's Office consider announcing the advertisement of a competitive bid procurement of credit monitoring services to calm fears regarding identity theft in the wake of the DOR breach and to ensure the best protection for citizens instead of entering into a contract with Experian with no competition, which is what was ultimately done?

4. Will DOR or the Governor's Office commit to ensuring a competitive bid process through the State procurement office will be followed for any future credit monitoring contract?

5. Were Citreas, IdentityForce or any other company considered, looked at (ex. viewed websites) or asked formally or informally to submit a bid for credit monitoring services before the October 25, 2012 contract with Experian was finalized? When were any other companies contacted?

6. By whom (on behalf of the State) were the companies considered for credit monitoring services contacted?

7. Who, on behalf of the State, led negotiation discussions with Experian? What was the role of Jon Nieditz in these discussions?

8. If the discussions were led by Nelson Mullins, by what means was Nelson Mullins authorized to lead these discussions? Was the authorization provided by the Governor's Office?

9. How did the cost of $12 Million evolve? Was this a cost proposed by Experian in a bid or a cost offered by the State?

10. The original October 25 contract with Experian was for 3.6 Million activation codes at a cost of $15.35 for the year per activation code. The maximum potential cost to the State under the original contract for one year could have been $55,260,000 if 3.6 Million taxpayers enroll in the credit monitoring services. Under the addendum to the contract, the maximum total cost to the State was capped at $12 Million. How was the $12 Million cost achieved?

11. What was the cost of HHS' contract with Experian following its recent breach? How many citizens were affected by that breach?

12. Are there any services being provided by Experian that the State has the capability to do now or that the State could provide at minimal additional cost? If yes, would handling any of these services "in house" reduce exposure of certain Personal Identifying Information?

13. Is there an itemization of the cost of each service being provided under the $12 Million contract with Experian? If no, what is the approximate value of each service being provided under the Experian contract?

14. After the end of the contract year with Experian, does the Governor's Office plan to have the State perform in house any of the functions currently being provided by Experian in order to reduce the cost to the State?

15. Experian stated that without a contract to extend its services for another year, it estimates 5-10% of taxpayers that enroll in Experian services under the contract with DOR will re-enroll for a second year. Based on a 5% re-enrollment, Experian estimates it will earn $5.2 Million in recurring revenue after the first year. Experian has stated it will enter into an extension of the contract with the State for an additional year for $10 Million. Given the disparity between the $5.2 Million Experian would normally earn after the first year of the hacking and the $10 Million offer, do you feel that a lower offer could be elicited from Experian or some other vendor through a competitive procurement process?

16. Given the disparity between the $12 Million contract for the first year and the $10 Million offer for second year services proposed just weeks after the initial contract was put in place, do you believe a contract amount of less than $12

Million could have been negotiated had the agreement been further negotiated or a competitive bid process were followed?

17. Mr. Kapcynski with Experian indicated that taxpayers who enroll in Experian's services under the South Carolina contract after November 29 will be notified immediately of the steps and the code necessary to enroll in "FamilySecure" if they qualify. How are these taxpayers being notified immediately if other taxpayers who enrolled before November 29 have not yet been notified? Experian has indicated that it will take through January to notify all eligible taxpayers of the "FamilySecure" product.

18. Some taxpayers enrolling as early as the end of October have not yet received the required notification to enroll in "FamilySecure." Experian told these taxpayers that they have no way of tracking who has been sent the notification, if the taxpayer's specific notification has been sent, or when a specific taxpayer will receive their notification. Essentially, Experian cannot tell an inquiring taxpayer whether their notification for FamilySecure has been sent, and does not have the ability to resend a notification in the event a taxpayer is not properly notified. Other taxpayers report that Experian has indicated that the FamilySecure notifications may be going to taxpayers' Junk e-mail box.

    How can the State and Experian ensure all eligible citizens receive the notification and code they need to enroll in the FamilySecure product?

19. Can the Governor's Office confirm that the same services were provided to HHS clients through Experian after its recent breach? How many people were affected by that breach? How many people signed up for Experian services under that contract? What was the cost of the Experian contract in that situation?

20. Why is there disparate treatment among equally impacted taxpayers regarding frequent access to credit reports? Taxpayers without dependants under the age of 18 are only entitled to one upfront credit report while taxpayers with young dependants are entitled to unlimited credit reports under FamilySecure.

21. Experian indicated that they are open to further negotiations to amend the existing contract, specifically relating to the ability for all taxpayers to access their credit reports frequently as is currently available for adults enrolled in the FamilySecure product. Has Nelson Mullins or the Governor's Office initiated further negotiations with Experian?

22. Does Nelson Mullins or the Governor's Office plan to request an extension of the January 31 contract deadline to enroll in Experian's services for free?

23. Has Nelson Mullins or the Governor's Office explored ways to auto-enroll citizens in the Experian product? Suggestions have included taxpayers authorize auto-enrollment as an option on their tax returns. (Experian said at the 12/13/12

hearing that it would see if this was an option. Has Experian reported its findings to the Governor's Office?

24. Experian has stated it is unable to auto-enroll citizens due to the verification process it has for enrollment into its programs. Is Experian unwilling to modify its standard sign-up process to allow for auto-enrollment based on the "list" DOR and the Governor's Office has provided to Experian or would such a modification to accommodate auto-enrollment of eligible citizens cost an additional amount?

25. If auto-enrollment would be an additional expense, what would this additional expense be?

26. Assuming that the Governor's Office plans to competitively bid for credit monitoring services after the year contract with Experian has expired, will the Governor's Office request bids from companies that can auto-enroll all eligible SC citizens?

II. Chernoff Newman Contract

1. What services has Chernoff Newman provided under its contract with the State?

2. Can a copy of the Chernoff Newman contract be provided?

3. Was any other company considered prior to entering into a contract with Chernoff Newman?

4. Why wasn't the contract with Chernoff Newman procured through the State Procurement Office? Was Chernoff Newman considered to be a "sole source" or the sole provider of the kind of services they offer?

5. Why was Chernoff Newman considered the "sole source" for public relations/communications services?

6. How long before the public was notified had Chernoff Newman been made aware of the breach? On what date was Chernoff Newman contacted by the State?

7. Why was Chernoff Newman contacted before notifying South Carolinians of the breach?

8. By whom was Chernoff Newman initially contacted?

9. On what date was the contract with Chernoff Newman finalized?

III. EMC Corporation

1. Is all data that was compromised in the DOR breach now encrypted?

2. What services have EMC Corporation provided to DOR or the State?

3. Does DOR or the State have a contract with EMC? If so, how was this contract procured? (Was a competitive process followed before contracting with EMC?

IV. General Questions Regarding DOR Breach

1. Which 18 agencies were inspected as part of the Inspector General's information security report?

2. IRS Publication 1075 contains requirements for computer security controls and tax information security guidelines for federal, state and local agencies. DOR has indicated that it was in compliance with the recommendations of the publication; however, the publication notes: "While the Safeguards Office has responsibility to ensure the protection of Federal Tax Information, it is the responsibility of the organization to build in effective security controls into their own Information Technology (IT) infrastructures to ensure that this information is protected at all points where Federal Tax Information (FTI) is received, processed, stored and/or maintained." While DOR may have complied with basic guidelines, it is apparent they did not build in effective security controls needed to fit the nuances of DOR particularly. Prior to the breach, were recommendations from IT professionals at DOR relayed to the DOR administration? Did the IT professionals within DOR fail to identify needs and recommendations altogether?

3. We have heard that a limitless number of cyber security technologies could be purchased to beef up the State's information security program; however, without proper employee training and implementation these technologies are prone to fail.

   What plan does the Governor's Office propose to ensure that employees are properly trained and implementing required security measures?

   If the Governor's Office proposes hiring a training firm for this purpose, will these services be competitively bid through the Procurement Office?

4. What are DSIT's capabilities in sending mass mailings/state notifications?

5. Did the Governor's Office consider DSIT for mailing out notices to the public instead of SourceLink or the other mailing/notification companies considered?

6. Why wasn't DSIT ultimately used to handle the mass mailing?