

State Information Technology Advisory Committee

December 11, 2012

1:00 PM – 3:00 PM

Dakota Carrier Network, Board Room

Members Present:

Lisa Feldner – Chair, Cory Fong, Laura Glatt, Tim Schenfisch for Bryan Klipfel, Alvin A. Jaeger, Maggie Anderson for Carol K. Olson, Peggy Link, Pam Sharp, Arvy Smith, Tom Trenbeath, and Grant Levi for Francis Ziegler

Members Absent: Sparb Collins, Maren Daley, Eric Hardmeyer, Sally Holewa, Representative Bob Skarphol, and Senator Larry Robinson

Others Present:

Jeff Quast, Gary Vetter, Mike Ressler, Dan Sipes, Doran Eberle, Duane Schell, Cher Thomas, Dean Glatt, and Russ Buchholz

Scribe:

Jeff Quast

Called to order at 1:08 PM, a quorum was present

Agenda / Topics discussed

Welcome – Lisa Feldner

Opening Comments – Jeff Quast

Mr. Quast reviewed the agenda and explained the emphasis on security for this meeting

EA Update – Cher Thomas

- Two requests for exemption to EGT003-04.6 from Commerce Dept. to use a modified web banner on mobile sites, will be reviewed by the ARB tomorrow
- Two request for exemption to AST003-05.5 from Commerce Dept. to use an alternative to the state login ID for two web applications/sites, will be reviewed by the ARB tomorrow
 - No technical reason have been defined, but ARB will look at the business side
- A request for exemption to OAT002-04.3 from Department of Financial Institutions to allow zip file attachments, will be reviewed by ARB tomorrow
 - 3 users that require data from the feds that only be sent via Email .zip attachments
 - Our newer management tools allow us to accommodate these kinds of requests
- One request for exemption to ST013-07.1 from the Public Service Commission to increase mobile device timeout, being reviewed by the ARB tomorrow
 - We can address this now with MDM so this will likely be approved
 - Some agencies will need the 5 minute limit, like AGOs office
- Anti-virus and Anti-malware standards were combined
 - Also added mobile device requirements
 - Some devices cannot run AV but are expected to run it as they become capable
- Multi-factor authentication

- Several agencies are working together to develop a solution
- Several different solutions are being considered
- New FBI requirements will make us use something by Q3 of 2013

ManTech Security Audit – Dan Sipes

- Results available upon request to the State Auditor’s Office

Mandan Data Center – Mike Ressler

- Are we comfortable with the location of the backup data center?
 - We have a good relationship with the power providers in both cities
 - No concerns about flooding at the Bismarck data center
 - A hot site at a location far away is cost prohibitive for bandwidth
 - Study showed that the only risk is sites located within 50 miles of each other
 - We are working with Montana to locate a backup data center there, but may be cost prohibitive
 - Of the sites reviewed, none have the needed capacity
 - Will keep the Mandan backup data center but continue to explore other locations/options
- Question from Ms. Glatt, does the extra space at UND work?
- Answer from Mr. Ressler, it is being looked at
- Question from Mr. Jaeger, is the 50 mile minimum a concern for tornadoes?
- Answer from Mr. Ressler, yes and other local threats/disasters. It is a balance of risk
- Question from Ms. Link, is there a cost of down-time? They justify spending the money up front to avoid downtime
- Answer from Mr. Ressler, yes, and that was the reason for upgrading the data center power supply. There is also High Availability in Mandan. Some agencies didn’t realize they didn’t have HA. Mr. Ressler asked agency leaders to think about what redundancy they have and need
- Question from Mr. Jaeger, how are the 2 locations are connected?
- Answer from Mr. Ressler, it is fiber, and there are two redundant links between Bismarck and Mandan

Mobile Device Management – Duane Schell

- We have a Mobile Device Management tool that was just installed
 - Allows us to improve the way we manage and support mobile devices
 - We used to use a lot of Blackberries which were built for the corporate market; now it is all iOS and Android devices and the tools are just catching up
 - We have 3 agencies using it and have several more interested
 - We have not publicized this yet as we still need to work out the initial issues

AppScan – Dan Sipes

- Web apps are increasingly used as an attack vector
- AppScan gives us the capability to scan web apps and find risks, which we can then fix or move that infrastructure and put it in an isolated zone
- We have been piloting it and looking at how we can scan our own apps
- It is not an insignificant task, you need someone who knows what they are doing
- If we find a problem with ITD or state developed apps we can fix them right away, whereas if it is a vendor app, we don’t have the same capability to require them to fix it
- This is just for web apps

Utah and SC Compromises – Dan Sipes

- Utah incident in March 2012
 - The issue was a default configuration on a server by a contractor

- South Carolina in August 2012
 - Spear phishing email, users gave up their credentials
 - The data they downloaded was encrypted but the hacker also got the encryption key and was able to decrypt it
 - MFA would have very likely prevented this breach
- ITD is reviewing its policies and controls to ensure we are doing everything we can
- Potential changes include MFA, encryption, enhanced logging and monitoring
- Will need to figure out how to fund, be it for unique agency solutions or for across the board
- We have a disaster recovery plan and security incident response team
- ITD is planning to work with agencies to develop a response plan and identify key roles and responsibilities
- Ms. Smith asked how concerned we should be about phishing emails
- Mr. Sipes answered that we need to do whatever we can to kill the emails
 - User awareness is key
 - Mr. Buchholz suggested that users need to notify the ITD service desk ASAP of phishing emails
- Mr. Fong added that developing a communications plan is a great idea and appreciates ITD's help in developing a response to questions they have received
- Mr. Sipes added that emails asking for state government credentials are the more important to us in securing our network than emails asking for personal credentials

Business Development Engine – Lisa Feldner

- Follow up on suggestion from Representative Skarphol at the last SITAC meeting to reintroduce the Business Development Engine project
- ITD has revised the quote for this and given it to OMB
- Ms. Sharp added that it was included in OMB's optional package
 - Narrative added that it was recommended by SITAC
 - It is not funded in the executive budget
 - Ms. Sharp intends to mention it at her testimony
 - Mr. Jaeger may have supporting material they could provide if needed
 - The real benefit would be to businesses, so there would need to be support from them

Wrap-up

Future Topics/ Closing Comments – Lisa Feldner

Adjournment – Lisa Feldner

- Dr. Feldner adjourned the meeting at 2:46 PM