



Presentation to the SITAC Meeting

December 11, 2012

**Dakota Carrier Network
Building**

Board Room



Agenda

- Welcome/Opening Comments
- Enterprise Architecture Update
- ManTech Security Report
- Mandan Data Center Update
- Mobile Device Management
- BREAK
- App Scan Services
- Utah and SC Compromises
- Business Development Engine
- Wrap-up



Lisa Feldner, CIO





Welcome and Opening Comments



**Jeff Quast,
Program
Administrator**

**Enterprise
Architecture**





Enterprise Architecture Update



Today's Theme - Security!

- Clear majority of EA topics and initiatives in the last 2 years have been security related
- Improved security requires resources
 - IT dollars
 - Inconvenience to users and citizens
 - Lost productivity
 - Increased complexity
- Little or no tangible ROI if nothing bad happens



**Cher Thomas,
Chairperson**

**Architecture Review
Board**





Enterprise Architecture Update



Requests for Exemption

- Two requests for exemption to EGT003-04.6 from Commerce Dept. and Ag Dept.
 - To use a modified web banner in mobile sites
- Two requests for exemption to AST003-05.5 from Commerce Dept.
 - To use an alternative to the State Login ID for two web applications/sites
- One request for exemption to OAT002-04.3 from Department of Financial Institutions
 - To allow .zip files as e-mail attachments for 3 users
- One request for exemption to ST013-07.1 from The Public Service Commission
 - To extend the timeout for some mobile devices to 15 minutes



Enterprise Architecture Update



Standards Updated

- The Anti-Virus and Anti-Malware standards were combined
 - <http://www.nd.gov/itd/standards/security/anti-virusmalware>
- The combined/updated standard now applies to Mobile Devices
 - Mobile Devices, **when able to**, must run Anti-Virus/Anti-Malware software
 - iOS devices are not currently considered able to run A-V/M software



Enterprise Architecture Update



Multi-Factor Authentication

- This has been studied and discussed for a long time
- Several agencies have deadlines of Q3-2013 to have a solution in place:
 - Dept. of Emergency Services, Attorney General's Office, ITD
 - Initial rollout to approximately 4,000 users
- ITD has started a project to provide an enterprise-level solution and offer it as a service, Charter nearing completion
- The use of MFA is expected to grow quickly and will likely become a standard or policy at some point
 - Federal Mandates
 - Effective (not perfect) defense against Phishing compromises
 - Passwords alone are simply no longer good enough



**Dan Sipes, Director
Administrative
Services**





ManTech Security Audit



- Results available upon request to State Auditor's Office



**Mike Ressler,
Deputy CIO**





Mandan Data Center

History

- 1988 – 2005 State contracted for Disaster Recovery service located out of state (mainframe & AS/400 only)
- 2005 – 2013 State leased data center space in Mandan from MDU (included mainframe, AS/400 and server based)
- 2012 Study options – ITD hired Sirius to conduct a “Business Continuity Planning and Recovery Site Evaluation”



Mandan Data Center

Findings

- | | |
|---|-------------------|
| General Facility Construction | - Meets Standards |
| Building Location (within 50 miles of Primary Data Center) | - Risk Exists |
| Building Location (ability for ITD staff to travel to facility) | - Advantage |
| Building Access Security | - Meets Standards |
| Power, Cooling, UPS, Backup Generator | - Meets Standards |
| Location Prone to Disasters | - Neutral |
| Affordable Network Connectivity | - Advantage |



Mandan Data Center

Cost Comparisons

Build New Backup Data Center	\$ 4,593,509 One-time
State of Montana DR Site / Miles City, MT	\$ 1,128,550 Annually
Mandan Data Center	\$ 94,980 Annually



**Duane Schell,
Director**

**Network Services
Division**





- Mobile Device Management
 - Solution to manage smartphone and tablets
 - Improve management
 - Improve security
 - Improve support
 - Targeted at Android and iOS devices
 - Migration away from Blackberry continues
 - Three agencies actively deploying
 - Several more interested



ZENPRISE





Break



**Dan Sipes, Director
Administrative
Services**





AppScan Update



- Security Processes
 - Assess
 - Protect (Prevent)
 - Detect
 - Respond
- Security Areas
 - Network Security
 - Host Security
 - Application Security
 - User Security
- Effective security will apply all four processes across all the security areas.



AppScan Update

- As the processes to secure networks and hosts have matured applications have become a more popular attack vector for hackers.
- Application security scanning is tied to the prevention principle.
 - We want to proactively identify risks in our applications and remediate or mitigate the risks before they are actively exploited.
 - We already have processes and tools in place to do this for the network and host layers of our security model.



AppScan Update

- ITD issued an RFP for an application scanning tool and made the award to IBM.
- Currently piloting the tool and plan to work with the ARB on recommendations for the following:
 - Funding model to recover costs for the staff and software necessary to perform the scanning and remediate identified risks.
 - Requirements for the proactive scanning of state developed and vendor developed applications.
 - Procedures for applications that cannot be remediated in a timely manner.



Utah and South Carolina Incidents

- Utah Incident - March 2012
 - 780,000 residents had PII, health data or social security numbers compromised.
 - Hackers, believed to be operating out of Eastern Europe, broke into a Medicaid server at the Utah Department of Health by exploiting a default password on server that had been configured by a contractor.
- South Carolina Incident
 - August 2012 a spear phishing attack containing malware resulted in compromised user credentials from at least one staff member from the SC Dept of Revenue.
 - September 2012 - attacker compromised 44 systems and exported 75 GB of encrypted and unencrypted data.



State Security Response Planning

- What is ITD doing
 - Reviewing existing Protect, Detect, Respond policies, controls and technologies to see if we need make any changes or additional investments.
- Potential Changes
 - Multi-Factor Authentication
 - Encryption
 - Enhanced logging and monitoring infrastructure
 - Identify funding mechanisms for any additional costs



State Security Response Planning

- Response Plan
 - ITD currently has a Disaster Recovery Plan and a Security Incident Response Team.
 - The State needs a more comprehensive plan and ITD is planning to work with key agencies to identify key roles and responsibilities in the event of a data breach.
- Items to Consider
 - Response Priority must be determined
 - Minimize customer impact
 - Identify and prosecute attackers
 - Restore operations quickly
 - Identify root cause vulnerability



State Security Response Planning

- Items to Consider - continued
 - Decide who will coordinate the frontline response.
 - What is the role of ITD beyond any technical response
 - What is the role of the agency affected
 - What is the role of the legal/risk management team
 - Who will coordinate with any external law enforcement entities
 - Who will function as the contact with the public and media
 - Determine what type of external assistance may be required to respond effectively and have existing contracts in place.
 - Define what constitutes a normal event versus major security incident.



Lisa Feldner, CIO





Wrap Up

- Closing comments
- Next meeting - June 2013
- Agenda items for next time?



THANK YOU!!!