ADOA
ARIZONA DEPARTMENT OF ADMINISTRATION

Information Technology Authorization Committee Review

August 27, 2014

ADOA-ASET: SPR Projects

Introductions:

- Jeffrey Crane

Presenters:

- Mike Lettman – CISO , ADOA-ASET
- Nancy Brister – EPMO Project Manager, ADOA-ASET

Projects:

- AD14001 – Security Assessments
- AD14010 – Central Cloud Security Management
- AD14004 – Data Center Security Management
- AD14007 – Data Center Management and Monitoring

Business Problem

- **Need for a comprehensive security strategy to protect State data and systems against emerging global security threats**

- *Example of Security Risks Identified on one day (8/6/14)*
  - 5 Incidents tracked
  - 11 MS-ISAC alerts received
  - 90,000 malicious email for ADOA dropped
  - 1,000,000 malicious web sites Statewide blocked
  - 1, 200,000,000 passwords/emails stolen by Russian hackers
- *Attacks prevented (8/6/14)*
  - 1 Heartbleed
  - 21 SQL Injections
  - 814 Trojans

Strategic Alignment and Risk

- Governor's Initiatives
  - Protect the State against threats to its systems and data

- ADOA – ASET's MBO
  - 1.4 Proactively Manage Enterprise Risk
    - 1.4.1 Implement Critical Business Continuity
    - 1.4.2 Enhanced Statewide Security and Privacy Capabilities

Proposed Solution:
AD14001 - Security Assessments

ADOA
ARIZONA DEPARTMENT OF ADMINISTRATION

Project Description:

- Perform Penetration Testing , Data Center Security Assessments, and define mitigation responses

What's Been Accomplished:

- FY13 - discovered and prioritized mission-critical State applications and data centers
- FY14 – completed identified security assessments and retested FY13 risks

What's Planned:

- Complete additional penetration testing, data center security assessments, and mitigation of FY14 findings

Benefits:

- Additional security assessments provide information to identify, prioritize, and mitigate security gaps on State applications and systems

***Questions*?**

Proposed Solution:
AD14004 - Data Center Security Management

ADOA
ARIZONA DEPARTMENT OF ADMINISTRATION

Project Description:

- Intrusion detection and response capabilities

What's Been Accomplished:

- Acquired compliance and analysis tools to correlate data and consolidate views into potential security threats
- Extended monitoring services to all internet access points
- Established a security operations center (SOC) to enhance intrusion detection

What's Planned:

- Implement additional intrusion detection technologies to further cybersecurity protections for the State

Benefits:

- Enhance and expand security for a more secure server operating environment

***Questions*?**

Proposed Solution:
AD14007 - Data Center Mgmt. and Monitoring

Project Description:

- Identify currently available firewall technologies to further protect the State from external threats to its systems and data.

What's Been Accomplished:

- Utilized security assessment data to address critical firewall security gaps
- Partnered with State agencies to evaluate firewall security protection requirements
- Completed Direct Proposal Request (DPR) procurement process to award a solution

What's Planned:

- Purchase, install, and implement Next Generation Firewall solution for ADOA and additional State agencies and entities

Benefits:

- Increase data security against internal and external threats in ADOA and support other State agencies where it does not currently exist

***Questions*?**

Proposed Solution:
AD14010 - Central Cloud Security Management

Project Description:

- Support “Cloud First” strategy though Cloud Application Protections and Cloud Security Management Services

What’s Been Accomplished:

- Researched, selected, and established web application firewalls, cloud firewalls, web content filtering solutions
- Advised on security as services were added to the cloud environment

What’s Planned:

- Expand cloud application protections for other State agencies and entities
- Provide security management as new services are added to the cloud

Benefits:

- Extend protections and security for ADOA-ASET's “Cloud First“ strategy

***Questions*?**