IT Security Update

University of Alaska
Board of Regents, December 12-13, 2013
Multi-factor authentication testing

• Additional level of security

• Works by delivering a unique 6 digit token that expires via phone, SMS or smartphone app login approval

• Security & IAM testing MFA for Single Sign On (SSO) enabled web apps and VPN
Adobe Breach Implications

- Adobe ID’s for ~3.8 million accounts breached in Oct. 2013
- Breach data published on Hacker site in Nov. 2013
- The data contained 2,114 UA email address as AdobeID usernames and their AdobeID password
- UA affiliated account holders were contacted and encouraged to change their UAusername password if it is the same as the one they used at Adobe
- To Date, NO UA system has been compromised
Ransomware Mitigations

- In October UAF & SW rolled out policies to mitigate the current wave of ransomware
- Coordinated with UAA & UAS to incorporate these into their environments
Closed External Audit Findings

• Implement central log collection and monitoring for all servers. Ensure that administrator access logging is configured. *A project to migrate existing services to the central log repository is underway, lead by OIT Security. OIT Security has draft service documentation out for review and comment.*

• Video monitoring or cardkey access to major network rooms: *existing controls adequate*
Closed External Audit Findings

• Implement password vault: provided outreach to staff via information security training, password management and guidance for tool selection

• Improve tracking of security activities: All OIT security activities are now tracked and managed through ticketing systems
OIT & UAA ITS are partnering to share knowledge and support investigation of copyright infringement claims through:

• sharing logging requirements
• sharing investigative workload
• Partnering with UAA Student Services for judicial action
Questions & Comments