

Cyber Security, the State Network and Identity Management

Frank Andrews, State Chief Security Officer

April 15, 2014

State Cyber Security Office



State Cyber Security Office

- Focal point for cyber security in state government
- Continuity of Operations training and support for over 900 users
- Conduct disaster recovery tests
- Physically protect the state data centers and Department of Information Systems
- Develop security rules for state government

CyberSecure
ARKANSAS



State Cyber Security Office

- Forensic investigations
- Advise agencies on security issues
- Coordinate external audits
- Deploy protective mechanisms for organizations on the state network
- Respond to restore communications during disasters

CyberSecure
ARKANSAS



“The Problem Space”

- **Security Operations:**
 - Policy management, Risk Assessment, Policy Negotiation, Privacy and Regulatory, Security Marketing
 - Risk Management, User Administration, Intrusion Detection, Operational Audit, Notification and Escalation
 - Forensics, Response, Capture, Recovery, Analysis
- **Security Enforcement:**
 - Physical Access, Business Processes, Applications, Systems, Networks



Arkansas State Network



What public entities are required by Arkansas Code to utilize the state network?

- State agencies
- Boards
- Commissions
- Higher education (administrative and business applications of information technology)
- K-12



What is the state network used for?

- Internet connectivity
- Data transmission
- Video conferencing
- Voice (Voice over Internet Protocol)



What is the scope of the state network?

- 3,067 circuits
- 2,130 addresses
- 2,059 network devices
- 2,024 routers provided by DIS including 1,712 customer edge routers
- 588 routers serving 1,081 school buildings in 238 out of 239 school districts



What security mechanisms are in place to help safeguard the state network?

- Maintain 1,100 firewalls
- Operate and maintain security information and event management (SIEM) system
- Intrusion prevention system
- State DNS infrastructure



Mobile Security



Mobile Security Reality

- Employees are accessing their work email via their work and personal phone
- Employees are downloading documents
- Mobile phone security measures are not mature
- Employees may be letting others use their mobile devices
- Mobile devices are frequently lost



Threats from Free Mobile Applications

- 401 percent more likely to track location and 314 percent more likely to access user address books than their paid counterparts
- 24.14 percent-permission to track user location
- 6.72 percent-permission to access user address books

Source: Juniper Networks' Mobile Threat Center analysis of over 1.7 million apps on the Google Play market from March 2011 to September 2012



Threats from Free Mobile Applications

- 2.64 percent-permission to silently send text messages
- 6.39 percent-permission to clandestinely initiate calls in the background
- 5.53 percent-permission to access the device camera
- Provide transport mechanisms for data transfer

Source: Juniper Networks' Mobile Threat Center analysis of over 1.7 million apps on the Google Play market from March 2011 to September 2012



BYOD (Bring Your Own Device)



BYOD

- You know people are bringing personal devices into your network and accessing business information
- In a 2012 SANS Mobile Device Survey only 9% of respondents felt completely aware of all mobile devices accessing their enterprise infrastructure and applications
- Do you know the extent of BYOD in your networks?



BYOD Security Concerns

- No password protection on the device
- No encryption
- Employees don't report loss
- Other applications pose a threat to your environment
- Security measures on phones aren't mature
- Wiping a personal phone deletes personal data too
- Phone can be subject to FOI
- Hundreds of different mobile device types



BYOD Security Measures

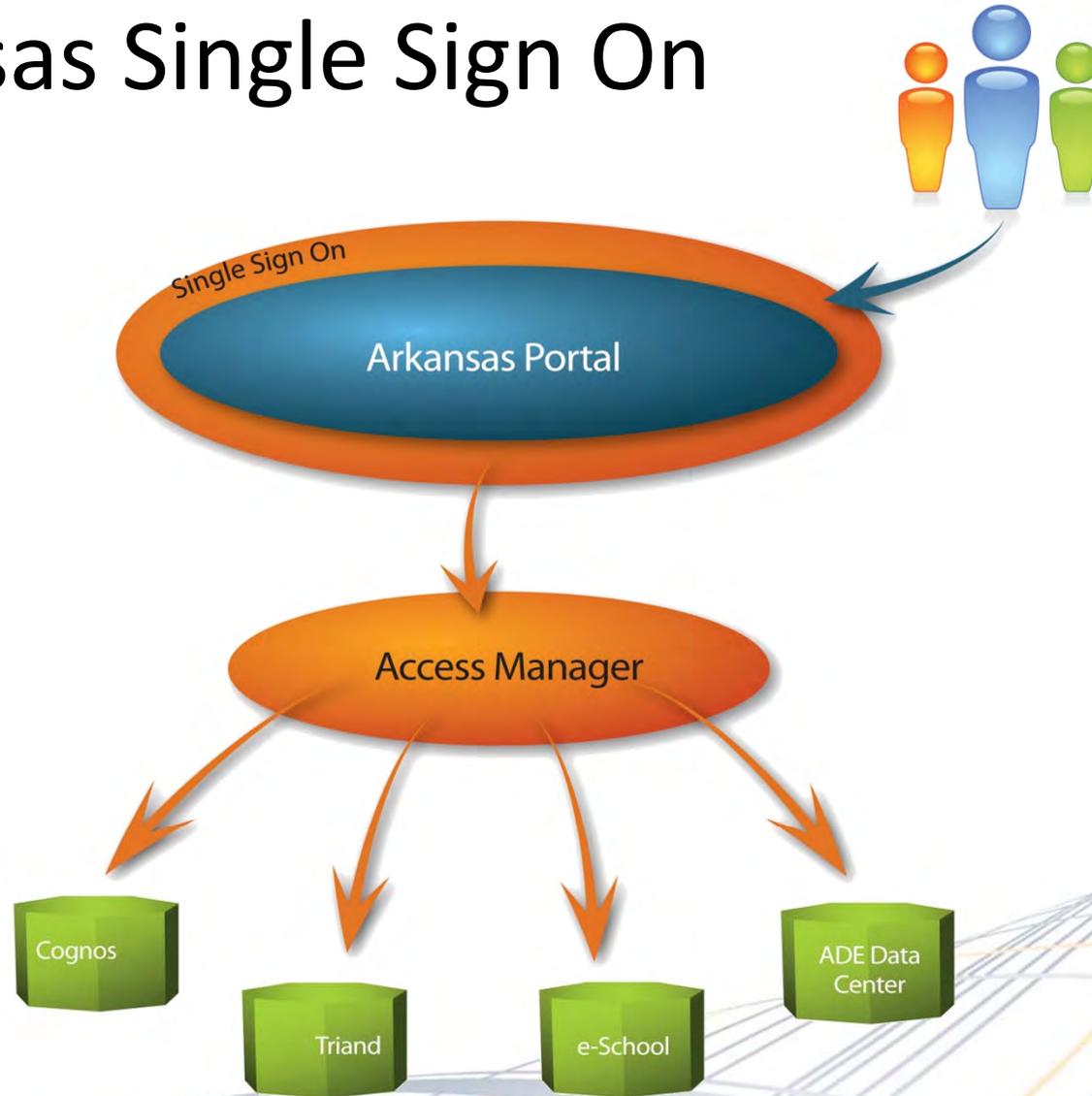
- BYOD policy signed by employee
- User education
- Mobile Device Management Software
 - Encrypt personal devices
 - Force security policies such as screen lock
 - Remote wipe
 - Capable of securing the mobile devices in your organization
 - Whitelist applications



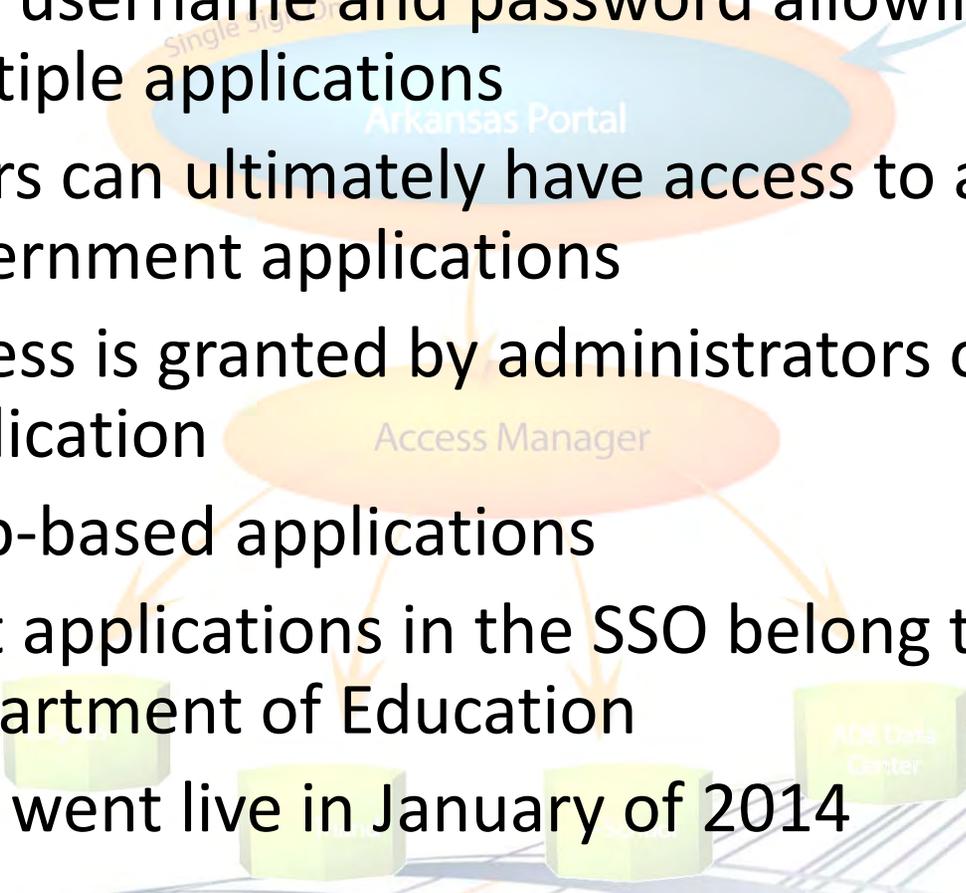
Identity Management



Arkansas Single Sign On



Arkansas Single Sign On

- Enterprise level single sign on solution 
 - One username and password allowing access to multiple applications
 - Users can ultimately have access to all kinds of government applications
 - Access is granted by administrators of each application
 - Web-based applications
 - First applications in the SSO belong to Arkansas Department of Education
 - SSO went live in January of 2014
- 

Questions?

Frank Andrews
State Chief Security Officer
franklin.andrews@arkansas.gov

