ARIZONA HOUSE OF REPRESENTATIVES

Fifty-sixth Legislature
First Regular Session

House: GOV DPA/SE 8-0-0-1 | 3rd Read 31-28-1-0
Senate: GOV DP 5-3-0-0 | 3rd Read 16-14-0-0
Final Pass: 31-27-1-0-1

HB 2416: ~~technical correction; sports facilities account~~
NOW: electronic applications; government employees; prohibition
Sponsor: Representative Gress, LD 4
Vetoed

Overview
Requires ADOA and AZDOHS to develop standards, guidelines and practices (Standards) for state agencies and contractors of this state (Agencies) for use of covered applications (Applications) on state information technology (IT) systems. Requires public institutions of higher education (Institutions) to develop Standards for the use of Applications.

History
ADOA is responsible for government IT functions (A.R.S. 18-102).

ADOA must develop, implement and maintain a coordinated state-wide plan for IT systems, including adopting statewide technical and coordination standards for IT (A.R.S. 18-104).

Provisions
1. Requires ADOA and AZDOHS, not more than 30 after the effective date, to develop Standards for Agencies that do the following:
   a) Require the removal of any Applications from state IT systems;
   b) Address the use of personal electronic devices by state employees and contractors of this state to conduct state business, including Application-enabled cell phones with remote access to an employee's state email account; and
   c) Identify sensitive locations, meetings or personnel within a state agency that could be exposed to covered applications-enable personal devices and develop restrictions on the use of personal cell phones, tablets or laptops in a designated sensitive location. (Sec. 1)
2. Requires each budget unit to develop policies to support the implementation of IT standards and report the policy to ADOA and AZDOHS. (Sec. 1)
3. Stipulates state employees and contractors may not:
   a) Conduct state business on any personal electronic device that has an Application;
   b) Use any communications equipment and services that are both of the following:
      i. Included on the Federal Communications Commission's covered communications equipment or services list; or
      ii. Used as a substantial or essential component of any system or as a critical technology as part of any system. (Sec. 1)
4. Requires each budget unit to implement network-based restrictions to prevent the use of prohibited technologies on budget unit networks by any electronic device and strictly enforce these restrictions. (Sec. 1)

☐ Prop 105 (45 votes) ☐ Prop 108 (40 votes) ☐ Emergency (40 votes) ☐ Fiscal Note

5. Requires each state employee to sign a document annually confirming the employee understands the IT systems Standards. (Sec. 1)

6. Stipulates a state employee who violates the Standards may be subject to disciplinary action, including termination of employment. (Sec. 1)

7. States ADOA, and AZDOHS, must require all state agencies and public institutions of higher education to implement security controls on state IT systems that do all of the following:
   a) Restrict access to application stores to prevent the installation of unauthorized applications;
   b) Can remotely disable non-compliant or compromised state IT systems;
   c) Can remotely uninstall unauthorized software from state IT systems;
   d) As necessary, deploy secure baseline configuration for state IT systems;
   e) Restrict access to any Application on all agency technology infrastructures and networks; and
   f) Restrict any personal electronic device that has an Application from connecting to agency technology infrastructures or state data. (Sec. 1)

8. Allows ADOA, and AZDOHS, to grant exemptions to the Standards to enable law enforcement investigations and other appropriate uses of Applications on state-issued devices if the state agency requesting access establishes a separate network. (Sec. 1)

9. States all exceptions to the information technology standards and guidelines must be reported to AZDOHS. (Sec. 1)

10. Outlines permissible exceptions to the IT Standards. (Sec. 1)

11. Requires Institutions, not more than 30 days after the effective date, to develop standards and submit them to AZDOHS and ADOA that do all of the following:
   a) Require the removal, and prohibit the installation of, any Application on IT that is owned and managed by the Institution;
   b) Restrict network access to prohibit downloading or accessing any Application using internet access provided by the Institution subject to specified exceptions;
   c) Require employees, students and other individuals who are provided access to information technology owned and managed by the Institution to acknowledge that IT owned and managed by the Institution may not be used to download or access an Application;
   d) Specify the limited exceptions for which the Institution will allow IT it owns and manages to be used to access Applications and the risk management actions that will be employed;
   e) Specifies exemptions may be granted if the use accomplishes one of the following:
      i. Are relevant to maintain the security of IT;
      ii. Relate to a criminal, civil or conduct investigation;
      iii. Relate to research or teaching; or
      iv. Involve sharing information with the public during an emergency. (Sec. 1)

12. Requires AZDOHS and ADOA to maintain the confidentiality of information developed and submitted to either department. (Sec. 1)

13. Requires ADOA and AZDOHS to annually update and publish a list of applications, services, hardware and software (IT system) that may be banned if the IT system presents a cybersecurity threat to Arizona. (Sec. 1)

14. Requires ADOA and AZDOHS to notify each state agency, JLBC, and OSPB directors of any IT system, including communications equipment and services, that is added to or removed from the list of potential cyber security threats. (Sec. 1)

15. Defines the following:
    a) *Contractor of this State;*
    b) *Company*;
    c) *Confidential or sensitive information*;
    d) *Country of concern*
    e) *Covered application*;
    f) *Public institution of higher education*;
    g) *Sensitive location*;
    h) *State business*;
    i) *State employee*; and
    j) *State information technology*. (Sec. 1)