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

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

Overview

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

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, 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 Agency to develop policies to support the implementation of IT standards and report the policy to ADOA. (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 (Equipment) that are included on the Federal Communications Commission's covered communications equipment or services list in accordance with the Secure and Trusted Communications Network Act of 2019;
   c) Use any Equipment that is deemed to pose an unacceptable risk to the national security of the United States. (Sec. 1)
4. Requires each Agency to implement network-based restrictions to prevent the use of prohibited technologies on agency 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 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 or unauthorized software repositories 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 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 or public institution of higher education 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. States a public institution of higher education may include an exception to accommodate students' use of a state email address on a device owned by the student or the student's immediate family. (Sec. 1)
12. Requires ADOA 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)
13. Requires ADOA to notify each state agency, public institution of higher education, the directors of JLBC and OSPB 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)
14. Defines the following:
   a) *Company*;
   b) *Confidential or sensitive information*;
   c) *Country of concern*
   d) *Covered application*;
   e) *Public institution of higher education*;
   f) *Sensitive location*;
   g) *State business*;
   h) *State employee*; and
   i) *State information technology*. (Sec. 1)

Senate Amendments

1. Adds the Arizona Department of Homeland Security (AZDOHS) to entities that must develop standards, guidelines and practices for state agencies and contractors that require, address and identify specified information technology subjects (Develop Standards).
2. Removes public institutions of higher education (Education Institutions) from entities that must

Develop Standards.

3. Redefines state agencies, state contractors and Education Institutions to *Budget Unit*.
4. Adds that state employees and contractors of the state may not use any communications equipment and services that are either:
   a) Included on the federal communications commission's covered communications equipment list; or
   b) Used as a substantial or essential component of any system or as a critical technology as part of any system.
5. Adds AZDOHS to the entities that must require all state agencies and Education Institutions to implement security controls on state information technology.
6. Removes the requirement to restrict access to *unauthorized software repositories*.
7. States AZDOHS may grant exceptions to enable law enforcement investigations.
8. Creates separate requirements for Education Institutions that require them to develop standards, guidelines and practices that do all the following:
   a) Require the removal of any covered application (Application) and prohibit the installation of any Application on IT that is owned by the Education Institution;
   b) Prohibit downloading Applications using internet access provided by the Education Institution;
   c) Require specified persons to acknowledge that IT owned by the Education Institution may not be used to download or access Applications; and
   d) Specify limitations the Education Institution will use to allow access to Applications. Exemptions must meet one of the following conditions:
      i. Are relevant to maintaining 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.
9. Requires AZDOHS and ADOA to maintain the confidentiality of all information received from specified entities.
10. Adds AZDOHS as an agency that must annually update and publish a list of applications that may be banned if it presents a cybersecurity threat to Arizona or the United States.
11. Stipulations AZDOHS and ADOA must notify each budget unit of any threats.
12. Defines *Contractor of this state*.
13. Redefines *Country of concern*.
14. Redefines *State business*.
15. Adds to the definition of *State employee*.
16. Adds to the definition of *State information technology*.