



ARIZONA HOUSE OF REPRESENTATIVES

Fifty-sixth Legislature
First Regular Session

House: GOV DPA/SE 8-0-0-1

HB 2416: technical correction; sports facilities account
S/E: electronic applications; government employees; prohibition
Sponsor: Representative Gress, LD 4
Caucus & COW

Summary of the Strike-Everything Amendment to HB 2416

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](#)).

Currently, ADOA must develop, implement and maintain a coordinated state wide plan for IT 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;
 - 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. Prohibits state employees and contractors of this state from conducting state business on any personal electronic device that has an Application. (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)
5. Requires each state employee to sign a document annually confirming the employee understands the IT Standers. (Sec. 1)
6. Stipulates a state employee who violates the Standards may be subject to disciplinary action, including termination of employment. (Sec. 1)

<input type="checkbox"/> Prop 105 (45 votes)	<input type="checkbox"/> Prop 108 (40 votes)	<input type="checkbox"/> Emergency (40 votes)	<input type="checkbox"/> Fiscal Note
--	--	---	--------------------------------------

7. States ADOA must require all state agencies and public institutions of higher education to implement security controls on state IT that does all of the following:
 - a) Restrict access to application stores or unauthorized software repositories to prevent the installation of unauthorized applications;
 - b) Have the ability to remotely disable noncompliant or compromised state IT;
 - c) Have the ability to remotely uninstall unauthorized software from state IT;
 - d) As necessary, deploy secure baseline configuration for state IT;
 - 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, service, 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 that is added to or removed from the list of potential cyber security threats. (Sec. 1)
14. Defines the following:
 - a) *Confidential or sensitive information*;
 - b) *Covered application*;
 - c) *Public institution of higher education*;
 - d) *Sensitive location*;
 - e) *State business*;
 - f) *State employee*; and
 - g) *State information technology*. (Sec. 1)