ARIZONA STATE SENATE

Fifty-Sixth Legislature, First Regular Session

FACT SHEET FOR H.B. 2416

~~technical correction; sports facilities account~~
(NOW: electronic government employees; prohibition)

Purpose

Establishes state information technology (IT) standards for state agencies, state contractors and public institutions of higher education and prescribes related prohibitions, restrictions and exceptions.

Background

The Arizona Department of Administration (ADOA) is responsible for government IT functions and must: 1) appoint a Chief Information Officer; 2) develop, implement and maintain a coordinated statewide IT plan; 3) formulate policies, plans and programs to effectuate ADOA's government IT purposes and adopt rules to further government IT objectives and programs; 4) accept, spend and account for grants, monies and direct payments and other grants of monies or property to conduct programs consistent with government IT purposes and objectives; 5) contract and enter into interagency and intergovernmental agreements with any public or private party; 6) establish an interactive online directory of codes, rules, ordinances and statutes to assist individuals and businesses with regulatory requirements and obligations; 7) manage enterprise-level IT infrastructure, except as specified, and develop strategies to protect IT infrastructure and its data; 8) temporarily suspend access to IT infrastructure when directed by the Arizona Department of Homeland Security (AZDOHS) and consult with the AZDOHS regarding security policies, standards and procedures; 9) provide staff support to the Information Technology Authorization Committee and report to the Committee on an annual basis; 10) require each budget unit to incorporate a life-cycle analysis into the IT planning, budgeting and procurement processes and to demonstrate expertise to carry out IT plans, as prescribed; 11) provide IT consulting services to budget units, advise each budget unit as necessary and maintain all confidential information received from a budget unit; 12) monitor IT projects considered to be major or critical and temporarily suspend expenditures if ADOA determines that the project is at risk of failing or does not comply with government IT requirements; 13) continuously study emergent technology and evaluate its impact on Arizona's system; 14) advise and make recommendations to the Governor and Legislature; and 15) have an official seal that must be judicially noticed (A.R.S. §§ 18-102; 18-103; and 18-121).

A *budget unit* is a department, commission, board, institution or other agency of the state receiving, expending or disbursing state funds or incurring obligations of the state, including the Arizona Board of Regents (ABOR) but excluding the universities under ABOR's jurisdiction, community college districts and legislative or judicial branches. *IT* is all computerized and auxiliary automated information processing, telecommunications and related technology, including hardware, software, vendor support and related services, equipment and projects (A.R.S. § 18-101).

There is no anticipated fiscal impact to the state General Fund associated with this legislation.

Provisions

State IT Standards

1. Requires ADOA to develop standards, guidelines and practices for state agencies, state contractors and public institutions of higher education that:
   a) require the removal of any covered application from state IT;
   b) address the use of personal electronic devices by state employees and contractors to conduct state business, including covered 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 application-enabled personal devices and develop restrictions on the use of personal cell phones, tablets or laptops in a designated sensitive location.

2. Specifies that ADOA must develop the standards, guidelines and practices no more than 30 days after the general effective date of this legislation.

3. Requires each state agency, state contractor and public institution of higher education to:
   a) develop a policy to support the implementation of the standards, guidelines and practices; and
   b) report the policy to ADOA.

4. Prohibits state employees and contractors from:
   a) conducting state business on any personal electronic device that has a covered application; and
   b) using any communications equipment and services that are included on the Federal Communications Commission's covered communications equipment or services list and deemed to pose an unacceptable risk to U.S. national security or the security and safety of U.S. citizens.

5. Requires each state agency, state contractor and public institution of higher education to:
   a) implement network-based restrictions to prevent the use of prohibited technologies on agency networks by any electronic device; and
   b) strictly enforce these restrictions.

6. Requires each state employee to sign a document annually confirming that the employee understands the prescribed standards, guidelines and practices.

7. Stipulates that a state employee who is found in violation of the prescribed standards, guidelines and practices may be subject to disciplinary action, including the termination of employment.

8. Directs ADOA to require all state agencies and public institutions of higher education to implement security controls on state IT that:
   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) deploys, as necessary, secure baseline configuration for state IT;

e) restrict access to any covered application on all agency technology infrastructures, including local networks, wide area networks and virtual private network connections; and
f) restrict any personal electronic device that has a covered application from connecting to agency technology infrastructures or state data.

Exceptions

9. Allows ADOA to grant exceptions to the state IT requirements to enable law enforcement investigations and other appropriate uses of covered applications on state-issued devices if the state agency or public institution of higher education requesting access establishes a separate network with the approval of the agency or institution head.

10. Prohibits, from being delegated, the approval of an agency or public institution of higher education head.

11. Requires a granted exception to be reported to AZDOHS.

12. Allows an exception to include:
    a) accomplishing a specific business need, such as enabling a criminal or civil investigation or sharing information to the public during an emergency; and
    b) for personal electronic devices, extenuating circumstances granted for a predetermined period of time.

13. Asserts that, to the extent practicable, exception-based usage should be performed only on a personal electronic device that is not used for other state business and on nonstate networks.

14. Requires, for exception-based use, cameras and microphones to be disabled on personal electronic devices.

15. Allows a public institution of higher education to include, in the IT policy submitted to ADOA, an exception to accommodate the student use of state email addresses provided by the institution.

16. Requires that any exception:
    a) is restricted to the student's use of a personal electronic device that is privately owned or leased by the student or a member of the student's immediate family; and
    b) includes network security considerations to protect the institution's network and data from traffic related to covered applications.

Notification Requirements

17. Requires ADOA to develop, annually update and publish a list of applications, services, communications equipment and services, and software that may be banned if the application, service, communications equipment and services, or software presents a cybersecurity threat to the state or the United States.

18. Requires ADOA to notify each state agency and public institution of higher education and the Directors of the Joint Legislative Budget Committee and Governor's Office of Strategic Planning and Budgeting of any application, service, communications equipment and services, or software that is added to or removed from the list.

Definitions

19. Defines *state IT* as including all state-issued and state-owned cell phones, laptops, tablets and desktop computers and any other state-issued and state-owned electronic devices that are capable of internet connectivity.

20. Defines a *covered application* as a social networking service and any current or future successor application or service developed or provided by a private company or any entity owned or operated by a private company that is founded, headquartered or located in a country of concern (CoC).

21. Defines a *CoC* as including China, Cuba, Eritrea, Iran, Myanmar, North Korea, Nicaragua, Pakistan, Russia, Saudi Arabia, Tajikistan and Turkmenistan.

22. Defines a *company* as an entity that:
    a) owns or operates, directly or indirectly, a platform that is directly or indirectly owned or operated by a CoC or is domiciled in, has its principal place of business in, is headquartered in or is organized under the laws of a CoC;
    b) is subjected to substantial control or influence, directly or indirectly, from a CoC;
    c) is directly or indirectly compelled to share data regarding U.S. citizens with a CoC; or
    d) uses software, communications equipment and services or an algorithm that is directly or indirectly controlled or monitored by a CoC.

23. Specifies, in the definition of *company*, that substantial control or influence of a CoC includes the content moderation practices of the entity that directly or indirectly owns or operates such a platform.

24. Defines a *public institution of higher education* as a university under the jurisdiction of ABOR or a community college.

25. Defines a *state employee* as including any full-time or part-time stat employee, a state contractor, a paid or unpaid state intern and any user of a state network.

26. Excludes, from the definition of *state employee*, a county, city or town employee.

27. Defines *state business* as the act of accessing any state-owned data or application, state email account, nonpublic facing communication, voice over internet protocol, short message service, videoconferencing and any other state database or application.

28. Defines *confidential or sensitive information* as including IT configurations, criminal justice information, financial data, personally identifiable data, sensitive personal information or any data protected by federal or state law.

29. Defines a *sensitive location* as any location, whether physical or electronic, that is used to discuss confidential or sensitive information, including video conferencing and electronic meetings rooms.

Miscellaneous

30. Becomes effective on the general effective date.

House Action

GOV	2/15/23	DPA/SE	8-0-0-1
3rd Read	2/28/23		31-28-1

Prepared by Senate Research
March 27, 2023
KJA/slp