ARIZONA STATE SENATE

Fifty-Sixth Legislature, First Regular Session

AMENDED

FACT SHEET FOR H.B. 2416

~~technical correction; sports facilities account~~

(NOW: electronic applications; government employees; prohibition)

Purpose

Requires the Arizona Department of Homeland Security (AZDOHS) and the Arizona Department of Administration (ADOA) to establish state information technology (IT) standards for state agencies and contractors and each public institution of higher education to establish IT standards, and prescribes related prohibitions, restrictions and exceptions.

Background

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 IT purposes and adopt rules to further 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 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 data; 8) temporarily suspend access to IT infrastructure when directed by AZDOHS and consult with AZDOHS regarding security policies, standards and procedures; 9) provide staff support to the IT Authorization Committee and annually report to the Committee; 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 the project is at risk of failing or does not comply with 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 AZDOHS and ADOA to develop standards, guidelines and practices for state agencies and contractors 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 AZDOHS and ADOA must develop the state IT standards no more than 30 days after the general effective date of this legislation.

3. Requires each budget unit to:
   a) develop a policy to support the implementation of the state IT standards and report the policy to AZDOHS and ADOA; and
   b) implement network-based restrictions to prevent the use of prohibited technologies on the budget unit's networks by any electronic device and strictly enforce these restrictions.

4. Prohibits state employees and contractors from conducting state business on any personal electronic device that has a covered application and from using any communications equipment and services that are:
   a) 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; and
   b) used as a substantial or essential component of any system or as a critical technology as part of any system.

5. Requires each state employee to sign a document annually confirming that the employee understands state IT standards.

6. Stipulates that a state employee who is found in violation of state IT standards may be subject to disciplinary action, including the termination of employment.

7. Directs AZDOHS and 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 to prevent the installation of unauthorized applications;
   b) have the ability to remotely disable noncompliant or compromised state IT and remotely uninstall unauthorized software from state IT;
   c) deploys, as necessary, secure baseline configuration for state IT;
   d) restrict access to any covered application on all agency technology infrastructures, including local networks, wide area networks and virtual private network connections; and
   e) restrict any personal electronic device that has a covered application from connecting to agency technology infrastructures or state data.

8. Allows AZDOHS and ADOA to grant exceptions to state IT standards to enable law enforcement investigations and other appropriate uses of covered applications on state-issued devices if the state agency requesting access establishes a separate network with the approval of the agency head.

9. Prohibits, from being delegated, the approval of an agency head.

10. 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.

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

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

13. Requires each granted exception to be reported to AZDOHS.

14. Requires AZDOHS and 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.

15. Requires AZDOHS and ADOA to notify each budget unit 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.

IT Standards for Public Institutions of Higher Education

16. Requires each public institution of higher education to develop and submit to AZDOHS and ADOA standards, guidelines and practices that:
    a) require the removal of any covered application from and prohibit the installation of any covered application on IT that is owned and managed by the public institution;
    b) restrict network access to prohibit downloading or accessing any covered application using internet access provided by the public institution;
    c) require employees, students and other individuals who are provided access to the public institution's IT to acknowledge, as a condition of obtaining access, that the IT may not be used to download or access a covered application; and
    d) specify the limited exceptions, if any, for which the public institution will allow IT to be used to access covered applications and the risk management actions that will be employed in connection with those uses.

17. Specifies that each public institution of higher education must develop the IT standards no more than 30 days after the general effective date of this legislation.

18. Requires an exception to the IT standards of a public institution to only be granted for uses that accomplish a specific need and that:
    a) are relevant to maintaining the security of IT;
    b) relate to research or teaching;
    c) relate to a criminal, civil or conduct investigation; or
    d) involve sharing information to the public during an emergency.

Miscellaneous

19. Requires AZDOHS and ADOA to maintain the confidentiality of information developed and submitted to either department that, if disclosed, could facilitate unauthorized access to IT systems, sensitive locations or sensitive or confidential information of the state, a state agency or a public institution of higher education.

20. 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, excluding electronic devices owned or managed by a public institution of higher education.

21. 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).

22. Defines a *CoC* as including any country included on the Federal Foreign Adversaries List.

23. 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.

24. Specifies, for 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.

25. Defines a *public institution of higher education* as a university under ABOR's jurisdiction or a community college.

26. Defines a *state employee* as including any full-time or part-time state employee, state contractor, paid or unpaid state intern or user of a state network, excluding:
    a) a county, city or town employee; or
    b) an employee of a public institution of higher education.

27. Defines *state contractor* as any entity that has entered into a contract to provide goods or services to any budget unit and whose contract requires the contractor and its employees to have access to state networks, excluding a public institution of higher education.

28. Defines *state business* as the act of accessing any state-owned nonpublic facing database or application.

29. Excludes, from the definition of *state business*, a database or application owned or managed by a public institution of higher education, including networks, email communication systems, voice over internet protocol, short message services and videoconfrencing.

30. 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.

31. 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.

32. Becomes effective on the general effective date.

<u>Amendments Adopted by Committee of the Whole</u>

1. Bifurcates the establishment of state IT standards for state agencies, state contractors and public institutions of higher education by ADOA into the establishment of:
   a) state IT standards for state agencies and contractors by AZDOHS and ADOA; and
   b) IT standards for public institutions by each public institution.

2. Requires AZDOHS, in addition to ADOA, to:
   a) receive the state IT policies of budget units;
   b) grant exceptions;
   c) develop, annually update and publish a list of applications, services, communications equipment and services, and software that may be banned and notify outlined entities of any change to the list; and
   d) require all state agencies and public institutions of higher education to implement security controls on state IT.

3. Removes restricting access to unauthorized software repositories from state IT security controls.

4. Prohibits state employees and contractors from using any communications equipment and services that are used as a substantial or essential component of any system or as a critical technology as part of any system.

5. Requires the IT standards of a public institution of higher education to:
   a) be developed no more than 30 days after the general effective date of this legislation;
   b) require the removal and prohibit the installation of any covered application;
   c) restrict network access to prohibit downloading or accessing any covered application;

d) require individuals who are provided access to IT to acknowledge, as a condition of obtaining access, that the IT may not be used to access a covered application; and
e) specify any limited exceptions and the risk management actions that will be employed.

6. Prescribes restrictions to granting a limited exception to a public institution's IT standards.

7. Requires AZDOHS and ADOA to maintain the confidentiality of information that, if disclosed, could facilitate unauthorized access to IT systems, sensitive locations or sensitive or confidential information, as specified.

8. Removes provisions that:
   a) allow a public institution of higher education to include an exception to accommodate the student use of state email addresses provided by the institution in an IT policy submitted to ADOA; and
   b) require any exception to be 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 to include network security considerations to protect the institution's network and data from traffic related to covered applications.

9. Defines *state contractor*.

10. Excludes, from the definition of:
    a) *state IT*, electronic devices owned or managed by a public institution of higher education; and
    b) *state employee*, an employee of a public institution of higher education.

11. Redefines a *CoC* as including any county included on the Federal Foreign Adversaries List, rather than China, Cuba, Eritrea, Iran, Myanmar, North Korea, Nicaragua, Pakistan, Russia, Saudi Arabia, Tajikistan and Turkmenistan.

12. Redefines *state business* to be the act of accessing any state-owned nonpublic facing database or application, rather than 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.

13. Adds exclusions to the definition of *state business*.

14. Makes conforming changes.

House Action				Senate Action			
GOV	2/15/23	DPA/SE	8-0-0-1	GOV	3/29/23	DP	5-3-0
3rd Read	2/28/23		31-28-1				

Prepared by Senate Research
May 8, 2023
KJA/slp