House Engrossed

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

State of Arizona
House of Representatives
Fifty-sixth Legislature
First Regular Session
2023

HOUSE BILL 2416

AN ACT

AMENDING TITLE 18, CHAPTER 1, ARTICLE 1, ARIZONA REVISED STATUTES, BY ADDING SECTION 18-105; RELATING TO STATE INFORMATION TECHNOLOGY.

(TEXT OF BILL BEGINS ON NEXT PAGE)

Be it enacted by the Legislature of the State of Arizona:

Section 1. Title 18, chapter 1, article 1, Arizona Revised Statutes, is amended by adding section 18-105, to read:

18-105. Cybersecurity threats; state information technology; standards; state employees and contractors; prohibition; exceptions; definitions

A. NOT MORE THAN THIRTY DAYS AFTER THE EFFECTIVE DATE OF THIS SECTION, THE DEPARTMENT SHALL DEVELOP STANDARDS, GUIDELINES AND PRACTICES FOR STATE AGENCIES, CONTRACTORS OF THIS STATE AND PUBLIC INSTITUTIONS OF HIGHER EDUCATION THAT DO ALL OF THE FOLLOWING:

1. REQUIRE THE REMOVAL OF ANY COVERED APPLICATION FROM STATE INFORMATION TECHNOLOGY.

2. ADDRESS THE USE OF PERSONAL ELECTRONIC DEVICES BY STATE EMPLOYEES AND CONTRACTORS OF THIS STATE TO CONDUCT STATE BUSINESS, INCLUDING COVERED APPLICATION-ENABLED CELL PHONES WITH REMOTE ACCESS TO AN EMPLOYEE'S STATE EMAIL ACCOUNT.

3. 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.

B. EACH STATE AGENCY, CONTRACTOR OF THIS STATE AND PUBLIC INSTITUTION OF HIGHER EDUCATION SHALL DEVELOP POLICIES TO SUPPORT THE IMPLEMENTATION OF THIS SECTION AND REPORT THE POLICY TO THE DEPARTMENT.

C. STATE EMPLOYEES AND CONTRACTORS OF THIS STATE MAY NOT:

1. CONDUCT STATE BUSINESS ON ANY PERSONAL ELECTRONIC DEVICE THAT HAS A COVERED APPLICATION.

2. USE ANY COMMUNICATIONS EQUIPMENT AND SERVICES THAT ARE INCLUDED ON THE FEDERAL COMMUNICATIONS COMMISSION'S COVERED COMMUNICATIONS EQUIPMENT OR SERVICES LIST PUBLISHED PURSUANT TO THE SECURE AND TRUSTED COMMUNICATIONS NETWORKS ACT OF 2019 (P.L. 116-124; 134 STAT. 158; 47 UNITED STATES CODE SECTION 1601) AND THAT ARE DEEMED TO POSE AN UNACCEPTABLE RISK TO THE NATIONAL SECURITY OF THE UNITED STATES OR THE SECURITY AND SAFETY OF UNITED STATES CITIZENS.

D. EACH STATE AGENCY, CONTRACTOR OF THIS STATE AND PUBLIC INSTITUTION OF HIGHER EDUCATION SHALL IMPLEMENT NETWORK-BASED RESTRICTIONS TO PREVENT THE USE OF PROHIBITED TECHNOLOGIES ON AGENCY NETWORKS BY ANY ELECTRONIC DEVICE. EACH STATE AGENCY, CONTRACTOR OF THIS STATE AND PUBLIC INSTITUTION OF HIGHER EDUCATION SHALL STRICTLY ENFORCE THIS SECTION.

E. EACH STATE EMPLOYEE SHALL SIGN A DOCUMENT ANNUALLY CONFIRMING THAT THE STATE EMPLOYEE UNDERSTANDS THE STANDARDS, GUIDELINES AND PRACTICES ADOPTED PURSUANT TO THIS SECTION. A STATE EMPLOYEE WHO IS FOUND TO HAVE VIOLATED THIS SECTION MAY BE SUBJECT TO DISCIPLINARY ACTION, INCLUDING TERMINATION OF EMPLOYMENT.

F. THE DEPARTMENT SHALL REQUIRE ALL STATE AGENCIES AND PUBLIC INSTITUTIONS OF HIGHER EDUCATION TO IMPLEMENT SECURITY CONTROLS ON STATE INFORMATION TECHNOLOGY THAT DO ALL OF THE FOLLOWING:

1. RESTRICT ACCESS TO APPLICATION STORES OR UNAUTHORIZED SOFTWARE REPOSITORIES TO PREVENT THE INSTALLATION OF UNAUTHORIZED APPLICATIONS.

2. HAVE THE ABILITY TO REMOTELY DISABLE NONCOMPLIANT OR COMPROMISED STATE INFORMATION TECHNOLOGY.

3. HAVE THE ABILITY TO REMOTELY UNINSTALL UNAUTHORIZED SOFTWARE FROM STATE INFORMATION TECHNOLOGY.

4. AS NECESSARY, DEPLOY SECURE BASELINE CONFIGURATION FOR STATE INFORMATION TECHNOLOGY.

5. RESTRICT ACCESS TO ANY COVERED APPLICATION ON ALL AGENCY TECHNOLOGY INFRASTRUCTURES, INCLUDING LOCAL NETWORKS, WIDE AREA NETWORKS, AND VIRTUAL PRIVATE NETWORK CONNECTIONS.

6. RESTRICT ANY PERSONAL ELECTRONIC DEVICE THAT HAS A COVERED APPLICATION FROM CONNECTING TO AGENCY TECHNOLOGY INFRASTRUCTURES OR STATE DATA.

G. THE DEPARTMENT MAY GRANT EXCEPTIONS TO THIS SECTION 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 HEAD OF THE AGENCY OR PUBLIC INSTITUTION OF HIGHER EDUCATION. THIS AUTHORITY MAY NOT BE DELEGATED. THE EXCEPTIONS DESCRIBED IN THIS SUBSECTION MUST BE REPORTED TO THE ARIZONA DEPARTMENT OF HOMELAND SECURITY. EXCEPTIONS MAY INCLUDE ANY OF THE FOLLOWING:

1. ACCOMPLISHING A SPECIFIC BUSINESS NEED, SUCH AS ENABLING A CRIMINAL OR CIVIL INVESTIGATION OR SHARING INFORMATION TO THE PUBLIC DURING AN EMERGENCY.

2. FOR PERSONAL ELECTRONIC DEVICES, EXTENUATING CIRCUMSTANCES GRANTED FOR A PREDETERMINED PERIOD OF TIME. TO THE EXTENT PRACTICABLE, EXCEPTION-BASED USAGE SHOULD BE PERFORMED ONLY ON PERSONAL ELECTRONIC DEVICES THAT ARE NOT USED FOR OTHER STATE BUSINESS AND ON NONSTATE NETWORKS. CAMERAS AND MICROPHONES MUST BE DISABLED ON PERSONAL ELECTRONIC DEVICES FOR EXCEPTION-BASED USE.

H. A PUBLIC INSTITUTION OF HIGHER EDUCATION MAY INCLUDE IN THE POLICY SUBMITTED TO THE DEPARTMENT AN EXCEPTION TO ACCOMMODATE THE USE BY STUDENTS OF A STATE EMAIL ADDRESS PROVIDED BY THE PUBLIC INSTITUTION OF HIGHER EDUCATION. ANY EXCEPTION SHALL 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 SHALL INCLUDE NETWORK SECURITY CONSIDERATIONS TO PROTECT THE PUBLIC INSTITUTION OF HIGHER EDUCATION'S NETWORK AND DATA FROM TRAFFIC RELATED TO COVERED APPLICATIONS.

I. THE DEPARTMENT SHALL 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 THIS STATE OR THE UNITED STATES. THE DEPARTMENT SHALL 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.

J. FOR THE PURPOSES OF THIS SECTION:

1. "COMPANY" MEANS AN ENTITY THAT MEETS ANY OF THE FOLLOWING:

(a) DIRECTLY OR INDIRECTLY OWNS OR OPERATES A PLATFORM THAT IS DIRECTLY OR INDIRECTLY OWNED OR OPERATED BY A COUNTRY OF CONCERN OR IS DOMICILED IN, HAS ITS PRINCIPAL PLACE OF BUSINESS IN, IS HEADQUARTERED IN OR IS ORGANIZED UNDER THE LAWS OF A COUNTRY OF CONCERN.

(b) IS SUBJECTED TO SUBSTANTIAL CONTROL OR INFLUENCE, DIRECTLY OR INDIRECTLY, FROM A COUNTRY OF CONCERN, INCLUDING THE CONTENT MODERATION PRACTICES OF THE ENTITY THAT DIRECTLY OR INDIRECTLY OWNS OR OPERATES SUCH A PLATFORM.

(c) IS DIRECTLY OR INDIRECTLY COMPELLED TO SHARE DATA REGARDING UNITED STATES CITIZENS WITH A COUNTRY OF CONCERN.

(d) USES SOFTWARE, COMMUNICATIONS EQUIPMENT AND SERVICES OR AN ALGORITHM THAT IS DIRECTLY OR INDIRECTLY CONTROLLED OR MONITORED BY A COUNTRY OF CONCERN.

2. "CONFIDENTIAL OR SENSITIVE INFORMATION" INCLUDES INFORMATION TECHNOLOGY CONFIGURATIONS, CRIMINAL JUSTICE INFORMATION, FINANCIAL DATA, PERSONALLY IDENTIFIABLE DATA, SENSITIVE PERSONAL INFORMATION OR ANY DATA PROTECTED BY FEDERAL OR STATE LAW.

3. "COUNTRY OF CONCERN" INCLUDES:

(a) CHINA.

(b) CUBA.

(c) ERITREA.

(d) IRAN.

(e) MYANMAR.

(f) NORTH KOREA.

(g) NICARAGUA.

(h) PAKISTAN.

(i) RUSSIA.

(j) SAUDI ARABIA.

(k) TAJIKISTAN.

(l) TURKMENISTAN.

4. "COVERED APPLICATION" MEANS 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.

5. "PUBLIC INSTITUTION OF HIGHER EDUCATION" MEANS A UNIVERSITY UNDER THE JURISDICTION OF THE ARIZONA BOARD OF REGENTS OR A COMMUNITY COLLEGE AS DEFINED IN SECTION 15-1401.

6. "SENSITIVE LOCATION":

(a) MEANS ANY LOCATION, WHETHER PHYSICAL OR ELECTRONIC, THAT IS USED TO DISCUSS CONFIDENTIAL OR SENSITIVE INFORMATION.

(b) INCLUDES VIDEO CONFERENCING AND ELECTRONIC MEETINGS ROOMS.

7. "STATE BUSINESS" INCLUDES THE ACT OF ACCESSING ANY STATE-OWNED DATA, STATE-OWNED APPLICATION, STATE EMAIL ACCOUNT, NONPUBLIC FACING COMMUNICATION, VOICE OVER INTERNET PROTOCOL, SHORT MESSAGE SERVICE, VIDEOCONFERENCING AND ANY OTHER STATE DATABASE OR APPLICATION.

8. "STATE EMPLOYEE":

(a) INCLUDES:

(i) ANY FULL-TIME OR PART-TIME EMPLOYEE OF THIS STATE.

(ii) A CONTRACTOR OF THIS STATE.

(iii) A PAID OR UNPAID INTERN OF THIS STATE.

(iv) ANY USER OF A STATE NETWORK.

(b) DOES NOT INCLUDE A COUNTY, CITY OR TOWN EMPLOYEE.

9. "STATE INFORMATION TECHNOLOGY" INCLUDES ALL STATE-ISSUED AND OWNED CELL PHONES, LAPTOPS, TABLETS AND DESKTOP COMPUTERS AND ANY OTHER STATE-ISSUED AND OWNED ELECTRONIC DEVICES THAT ARE CAPABLE OF INTERNET CONNECTIVITY.