BILL ANALYSIS

Senate Research Center
88R11862 YDB-D

S.B. 2358
By: Parker
Business & Commerce
4/14/2023
As Filed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

S.B. 2358 was drafted in response to increased concerns about foreign and domestic actors that use data derived from digital applications to undermine the security of the Texas government and its residents. The purpose of the bill is to provide the Department of Information Resources (DIR) with the authority to determine if a digital application may undermine the security of the state by collecting information from users and using that information in a malicious manner. DIR would then work with state agencies to ban or limit the use of those applications on state devices and personal devices used in the workplace.

As proposed, S.B. 2358 amends current law relating to security procedures for digital applications that pose a network security risk to state agencies.

RULEMAKING AUTHORITY

Rulemaking authority is expressly granted to the Department of Information Resources in SECTION 1 (Section 2054.626, Government Code) of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Chapter 2054, Government Code, by adding Subchapter S, as follows:

SUBCHAPTER S. DIGITAL APPLICATION SECURITY PROCEDURES

Sec. 2054.621. DEFINITIONS. Defines "digital application," "network security," and "user."

Sec. 2054.622. DIGITAL APPLICATION SECURITY RISK LIST. Requires the Department of Information Resources (DIR) to:

(1) compile, maintain, and annually update a list of digital applications that create a network security risk to state agencies;

(2) limit or prohibit the placement and use of digital applications on the list under Subdivision (1) on:

(A) state-owned cell phones, computers, and other communication devices; and

(B) personal communication devices of state agency employees that are used in the agency's office or other workplace; and

(3) post the list under Subdivision (1) on a publicly accessible web page on DIR's Internet website.

Sec. 2054.623. DIGITAL APPLICATION SECURITY MODEL POLICY FOR STATE AGENCIES. Requires DIR to develop, maintain, and periodically update a model policy for state agencies to use under Section 2054.624 in limiting or prohibiting the placement

and use on communication devices of the digital applications included on the list compiled under Section 2054.622.

Sec. 2054.624. STATE AGENCY DIGITAL APPLICATION SECURITY POLICY. (a) Requires each state agency to develop, implement, and periodically update a policy limiting or prohibiting the placement and use of digital applications included on the list compiled under Section 2054.622 on:

(1) state-owned cell phones, computers, and other communication devices; and

(2) personal communication devices of state agency employees that are used in the agency's office or other workplace.

(b) Requires each state agency to submit to DIR a copy of the policy required under Subsection (a) and updates to the policy.

(c) Provides that DIR:

(1) is authorized to offer recommendations for improvements to submitted policies;

(2) is required to retain each copy and update submitted under Subsection (b); and

(3) is required to notify each member of the legislature and the governor when a state agency submits a policy or update.

Sec. 2054.625. DISCLOSURE EXEMPTION. Provides that the model policy and state agency policies developed under this subchapter are exempt from disclosure under Chapter 552 (Public Information).

Sec. 2054.626. RULEMAKING AUTHORITY. Authorizes DIR to adopt rules to implement this subchapter.

SECTION 2. (a) Requires DIR, as soon as practicable after the effective date of this Act, but not later than January 1, 2024, to develop the digital application security risk list and model policy as required by Subchapter S, Chapter 2054, Government Code, as added by this Act.

(b) Provides that a state agency is not required to comply with Section 2054.624, Government Code, as added by this Act, until May 1, 2024.

SECTION 3. Effective date: September 1, 2023.