HOUSE FLOOR AMENDMENT EXPLANATION

Bill Number: **HB2736**

Kolodin Floor Amendment

- Changes the data encryption and cybersecurity pilot program to a study.
- Directs the assessing entity to identify the needs and solutions for specific entities and requests model implementation legislation.
- Strikes cybersecurity audit requirements that require and audit to be conducted in accordance with specified laws and policies.
- Requires audit results to be made publicly available 48 hours after completion.
- Specifies that source code is only to be able to be reviewed by the Auditor General.

Amendment explanation prepared by Tasja M
Phone Number 63476
ls
3/10/2025

ADDITIONAL COW
KOLODIN FLOOR AMENDMENT
HOUSE OF REPRESENTATIVES AMENDMENTS TO H.B. 2736
(Reference to House engrossed bill)

Amendment instruction key:
[GREEN UNDERLINING IN BRACKETS] indicates text added to statute or previously enacted session law.
[Green underlining in brackets] indicates text added to new session law or text restoring existing law.
[~~GREEN STRIKEOUT IN BRACKETS~~] indicates new text removed from statute or previously enacted session law.
[~~Green strikeout in brackets~~] indicates text removed from existing statute, previously enacted session law or new session law.
<<Green carets>> indicate a section added to the bill.
<<~~Green strikeout in carets~~>> indicates a section removed from the bill.

The bill as proposed to be amended is reprinted as follows:

Section 1. Title 26, chapter 1, article 1, Arizona Revised Statutes, is amended by adding section 26-108, to read:

26-108. Cybersecurity assessments; audits; requests; authorization; procedures

A. ON REQUEST OF THE [~~DEPARTMENT OF ADMINISTRATION OR ANY AGENCY THAT IS PART OF THE EXECUTIVE BRANCH OF GOVERNMENT OR ON THE REQUEST OF THE~~] LEGISLATIVE BRANCH OF GOVERNMENT, THE DEPARTMENT OF EMERGENCY AND MILITARY AFFAIRS CYBERSECURITY TEAM SHALL CONDUCT AN ASSESSMENT OF ANY TECHNOLOGY PRODUCT THAT IS OR MAY BE PURCHASED BY [~~THE REQUESTING ENTITY~~][A GOVERNMENT AGENCY].

B. THE CYBERSECURITY TEAM MAY PERFORM THE FOLLOWING SECURITY EVALUATION DURING AN ASSESSMENT PURSUANT TO SUBSECTION A OF THIS SECTION:

1. PENETRATION TESTING TO IDENTIFY VULNERABILITIES AND ASSESS THE ROBUSTNESS OF CYBERSECURITY DEFENSES.

2. HARDWARE NONDESTRUCTIVE TESTING TO EVALUATE THE INTEGRITY AND SECURITY COMPLIANCE OF PHYSICAL TECHNOLOGY COMPONENTS.

3. VENDOR-CAPABILITY VERIFICATION TO CONFIRM THAT A VENDOR THAT CONTRACTS WITH THE [~~REQUESTING ENTITY~~][GOVERNMENT AGENCY] IS ABLE TO MEET A CONTRACT'S TECHNICAL OBLIGATIONS AND CYBERSECURITY STANDARDS.

C. BEFORE THE [~~REQUESTING ENTITY~~][GOVERNMENT AGENCY] MAKES A PROCUREMENT DETERMINATION TO PURCHASE A TECHNOLOGY PRODUCT, THE CYBERSECURITY TEAM MAY CONDUCT AN AUDIT, SECURITY REVIEW AND COMPLIANCE VERIFICATION FOR THE [~~ENTITY~~][GOVERNMENT AGENCY]. THE [~~REQUESTING ENTITY~~][GOVERNMENT AGENCY] MAY HAVE THE CYBERSECURITY TEAM CONDUCT AN AUDIT TO ASSESS THE COST FOR THE ENTITY TO PURCHASE AND USE A DATA ENCRYPTION SYSTEM ON ALL OF THE ENTITY'S INFORMATION TECHNOLOGY SYSTEMS.

D. [~~A CYBERSECURITY AUDIT MUST BE CONDUCTED IN ACCORDANCE WITH BOTH OF THE FOLLOWING:~~

~~1. ALL STATE AND FEDERAL LAWS, INCLUDING THE UNITED STATES DEPARTMENT OF DEFENSE INSTRUCTION 1100.24, THAT ALLOW THE UNITED STATES DEPARTMENT OF DEFENSE AND THE DEPARTMENT OF EMERGENCY AND MILITARY AFFAIRS TO INTERFACE WITH A CIVILIAN ENTITY FOR INFRASTRUCTURE AND TECHNOLOGY SUPPORT.~~

~~2. ALL CYBERSECURITY POLICIES AND BUDGET CONSIDERATIONS THAT ENSURE THAT THE DEPARTMENT OF EMERGENCY AND MILITARY AFFAIRS ENSURES THAT RESOURCES ARE ALLOCATED EFFICIENTLY TO SUPPORT THE SECURITY AND INTEGRITY OF PROCURING TECHNOLOGY IN THIS STATE~~][THE RESULTS OF THE AUDIT SHALL BE MADE AVAILABLE TO THE PUBLIC ON THE DEPARTMENT'S WEBSITE WITHIN FORTY-EIGHT HOURS AFTER THE AUDIT'S COMPLETION].

Sec. 2. Data encryption and cybersecurity study; implementation and system requirements; audit and testing; reports; delayed repeal

A. The Arizona department of homeland security shall implement a seven-year data encryption and cybersecurity [~~pilot program~~][study] that is designed to protect information technology data against unauthorized access through the use of a software and hardware solution and to upgrade the cybersecurity infrastructure of information technology systems in this state.

B. In fiscal year 2025-2026, if monies are appropriated for this [~~pilot program~~][study], the Arizona department of homeland security shall create a plan, choose a vendor and begin the seven-year [~~pilot program~~][study]. The [~~pilot program~~][study] shall be implemented by the following entities in the following fiscal years:

1. In fiscal year 2026-2027, the [~~secretary of state~~][assessing entity] shall [~~implement a data encryption system and upgrade~~][perform a study of] the cybersecurity [~~infrastructure~~][needs] of the secretary of state's office[and prepare a report with proposed solutions, cost estimates, and model implementing legislation, for review by the president of the Senate, the speaker of the House of Representatives and the House of Representatives and Senate committees with jurisdiction over elections].

2. In fiscal year 2027-2028, the [~~department of revenue~~][assessing entity] shall [~~implement a data encryption system and upgrade~~][perform a study of] the cybersecurity [~~infrastructure~~][needs] of the department[of revenue and prepare a report with proposed solutions, cost estimates, and model implementing legislation, for review by the president of the Senate, the speaker of the House of Representatives and the House of Representatives and Senate committees with jurisdiction over taxation].

3. In fiscal year 2028-2029, the [~~department of administration~~][assessing entity] shall [~~implement a data encryption system and upgrade~~][perform a study of] the cybersecurity [~~infrastructure~~][needs] of the department[of administration and prepare a report with proposed solutions, cost estimates, and model implementing legislation, for review by the president of the Senate, the speaker of the House of Representatives and the House of Representatives and Senate committees with jurisdiction over state government].

4. In fiscal year 2029-2030, the [~~legislature~~][assessing entity] shall [~~implement a data encryption system and upgrade~~][perform a study of] the cybersecurity [~~infrastructure~~][needs] of the legislature[and prepare a report with proposed solutions, cost estimates, and model implementing legislation, for review by the president of the Senate and the speaker of the House of Representatives].

C. [~~The~~][Any proposed] data encryption system must meet all of the following criteria:

1. Have source code that is [only] accessible for review and audit by the auditor general.

2. Be owned by this state.

3. Be created and maintained by a company located in the United States that is only owned by United States citizens and has no foreign owners or investors.

4. Have a shareable code for transparency and audit purposes[that is accessible for review and audit by the auditor general].

5. Have a key-connected password system that is quantum encryption proof or future proof to other encryption breaking methodologies.

6. Be encryption agnostic. For the purposes of this paragraph, "encryption agnostic" means the system can use any encryption as long as the encryption can follow key-connected passwords.

7. Be able to reset, including password resets, without having to go to a third party for key resetting.

8. Have an audit trail for any key reset.

9. Have a master key that can be exchanged or recreated on demand with a signed and encrypted audit trail for all changes.

10. Allow each key package to contain a signed and encrypted audit trail.

11. Use technology that is protected by a unique United States patent.

12. Have United States department of defense-level security that is evidenced by penetration testing. For the purposes of this paragraph, "penetration testing" means a simulated cyber attack that is authorized to evaluate the security of the system.

13. Be purchased from a vendor that:

(a) Collaborates with the state agency that is implementing the encryption system to ensure seamless integration and compliance with all state and federal cybersecurity standards.

(b) Provides a United States-sourced encryption system.

(c) Is located and managed in the United States by United States citizens and that does not have any foreign owners or investors.

(d) Possesses a unique United States patent for the encryption system.

D. The auditor general may audit the encryption system at each stage of the implementation and operation of the data encryption system. After the implementation of the data encryption system is complete, the auditor general shall conduct an annual audit for seven years beginning in fiscal year 2026-2027 to ensure ongoing compliance with security standards and to identify potential security vulnerabilities with the data encryption system.

E. The Arizona department of homeland security shall submit to the legislature an annual report beginning in fiscal year 2026-2027 and continuing for five additional fiscal years. The report must include the status of the data encryption system implementation, the results of any security assessments that were completed and whether any implementation or operation issues were encountered in the previous year. In fiscal year 2031-2032, the Arizona department of homeland security shall submit a final report to the legislature that summarizes the overall effectiveness and security of the data encryption system.

F. This section is repealed from and after June 30, 2034.

ALEXANDER KOLODIN

2736FloorKOLODIN1.docx
03/10/2025
09:36 AM
C: SP