HOUSE FLOOR AMENDMENT EXPLANATION

Bill Number: **HB 2736**

Gillette Floor Amendment

- Allows the Department of Administration or any agency that is apart of the Executive Branch or the request of the Legislative Branch or the Department of Emergency and Military Affairs Cybersecurity Team to conduct an assessment of any technology product.
- Outlines evaluations that the cybersecurity security evaluation team may perform.
- Allows the cybersecurity team to conduct certain verifications for the requesting entity before the entity purchases a technology product.
- Requires a cybersecurity audit to be conducted in accordance with specified laws and standards.
- Transfers the data encryption and cybersecurity pilot program from the Department of Administration to the Arizona Department of Homeland Security.
- Extends the pilot program from five to seven years.
- Strikes the appropriation section.

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

GILLETTE FLOOR AMENDMENT
HOUSE OF REPRESENTATIVES AMENDMENTS TO H.B. 2736
(Reference to printed 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.

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 IS ABLE TO MEET A CONTRACT'S TECHNICAL OBLIGATIONS AND CYBERSECURITY STANDARDS.

C. BEFORE THE REQUESTING ENTITY MAKES A PROCUREMENT DETERMINATION TO PURCHASE A TECHNOLOGY PRODUCT, THE CYBERSECURITY TEAM MAY CONDUCT AN AUDIT, SECURITY REVIEW AND COMPLIANCE VERIFICATION FOR THE ENTITY. THE REQUESTING ENTITY 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.]>>

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

A. The [Arizona] department of [~~administration~~] [homeland security] shall implement a [~~five-year~~] [seven-year] data encryption and cybersecurity pilot program 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,] the [Arizona] department of [~~administration~~] [homeland security] shall create a plan, choose a vendor and begin the [~~five-year~~] [seven-year] pilot program. The pilot program shall be implemented by the following entities in the following fiscal years:

1. In fiscal year 2026-2027, the secretary of state shall implement a data encryption system and upgrade the cybersecurity infrastructure of the secretary of state's office.

2. In fiscal year 2027-2028, the department of revenue shall implement a data encryption system and upgrade the cybersecurity infrastructure of the department.

3. In fiscal year 2028-2029, the department of administration shall implement a data encryption system and upgrade the cybersecurity infrastructure of the department.

4. In fiscal year 2029-2030, the legislature shall implement a data encryption system and upgrade the cybersecurity infrastructure of the legislature.

C. The data encryption system must meet all of the following criteria:

1. Have source code that is 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.

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 [~~five~~] [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 [~~administration~~] [homeland security] shall submit to the legislature an annual report beginning in fiscal year 2026-2027 and continuing for [~~four~~] [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 [~~2030-2031~~] [2031-2032], the [Arizona] department of [~~administration~~] [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, [~~2032~~] [2034].

~~<<Sec. 3. Appropriations; department of administration; data encryption system; cybersecurity infrastructure~~

~~The sum of $_____ is appropriated from the state general fund in each of fiscal years 2025-2026, 2026-2027, 2027-2028, 2028-2029 and 2029-2030 to the department of administration for planning, purchasing and implementing a data encryption system and upgrading the cybersecurity infrastructure of information technology systems in this state.>>~~

Enroll and engross to conform
Amend title to conform

JOHN GILLETTE

2736FloorGILLETTE.docx
03/03/2025
12:26 PM
C: SP