REFERENCE TITLE: cybersecurity; data encryption; pilot program

State of Arizona
House of Representatives
Fifty-seventh Legislature
First Regular Session
2025

# HB 2736

Introduced by
Representatives Gillette: Biasiucci, Bliss, Carter N, Hendrix, Martinez, Nguyen, Travers, Volk, Way, Wilmeth; Senators Angius, Fernandez, Gowan, Kavanagh, Payne

AN ACT

ESTABLISHING A DATA ENCRYPTION AND CYBERSECURITY PILOT PROGRAM; APPROPRIATING MONIES.

(TEXT OF BILL BEGINS ON NEXT PAGE)

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

Section 1. Data encryption and cybersecurity pilot program; implementation and system requirements; audit and testing; reports; delayed repeal

A. The department of administration shall implement a five-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, the department of administration shall create a plan, choose a vendor and begin the five-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 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 department of administration shall submit to the legislature an annual report beginning in fiscal year 2026-2027 and continuing for four 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, the department of administration 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.

Sec. 2. 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.