House Engrossed

statewide cybersecurity encryption system; requirements

State of Arizona
House of Representatives
Fifty-seventh Legislature
Second Regular Session
2026

HOUSE BILL 2809

AN ACT

AMENDING TITLE 18, CHAPTER 5, ARIZONA REVISED STATUTES, BY ADDING ARTICLE 5; RELATING TO NETWORK SECURITY.

(TEXT OF BILL BEGINS ON NEXT PAGE)

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

Section 1. Title 18, chapter 5, Arizona Revised Statutes, is amended by adding article 5, to read:

ARTICLE 5. POST-QUANTUM ENCRYPTION SYSTEMS

18-561. Definitions

IN THIS ARTICLE, UNLESS THE CONTEXT OTHERWISE REQUIRES:

1. "CMMC 2.0" MEANS THE CYBERSECURITY MATURITY MODEL CERTIFICATION VERSION 2.0 THAT IS ESTABLISHED BY THE UNITED STATES DEPARTMENT OF DEFENSE.

2. "POST-QUANTUM ENCRYPTION" MEANS CRYPTOGRAPHIC ALGORITHMS THAT ARE DESIGNED TO BE SECURE AGAINST BOTH CLASSICAL AND QUANTUM COMPUTATIONAL ATTACKS, INCLUDING ALGORITHMS THAT EXCEED STANDARDS IDENTIFIED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY IN THE UNITED STATES DEPARTMENT OF COMMERCE.

3. "STATE AGENCY" HAS THE SAME MEANING PRESCRIBED IN SECTION 18-422.

4. "VENDOR" MEANS A PRIVATE ENTITY THAT PROVIDES CYBERSECURITY SOFTWARE, HARDWARE OR SERVICES PURSUANT TO A CONTRACT WITH THIS STATE.

18-562. Statewide post-quantum cybersecurity system; implementation; procurement

A. THIS STATE SHALL IMPLEMENT A STATEWIDE CYBERSECURITY SYSTEM THAT USES POST-QUANTUM ENCRYPTION THAT MEETS OR SURPASSES A COMPLETED INITIAL CMMC 2.0 VALIDATION.

B. THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM SHALL BE DEPLOYED ACROSS EACH STATE AGENCY THAT PROCESSES, STORES OR TRANSMITS ANY OF THE FOLLOWING:

1. PERSONAL IDENTIFYING INFORMATION.

2. SENSITIVE STATE DATA.

3. DATA RELATED TO ELECTIONS, PUBLIC SAFETY, PUBLIC BENEFITS, FINANCE OR INFRASTRUCTURE.

4. ANY DATA THAT IS DESIGNATED AS CONFIDENTIAL BY A STATE OR FEDERAL LAW.

C. THE PROCUREMENT OF THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM MUST BE CONDUCTED IN ACCORDANCE WITH TITLE 41, CHAPTER 23. ANY ELIGIBLE VENDOR MUST MEET ALL OF THE FOLLOWING QUALIFICATIONS:

1. BE A ONE HUNDRED PERCENT UNITED STATES-BASED COMPANY.

2. USE SOFTWARE, HARDWARE AND CRYPTOGRAPHIC COMPONENTS THAT ARE DEVELOPED, MANUFACTURED AND MAINTAINED EXCLUSIVELY IN THE UNITED STATES.

3. MEET OR EXCEED THE UNITED STATES DEPARTMENT OF DEFENSE CYBERSECURITY STANDARDS.

4. NOT HAVE A PARENT COMPANY, SUBSIDIARY, DEVELOPMENT PARTNER OR DATA DEPENDENCY THAT IS LOCATED OUTSIDE OF THE UNITED STATES.

D. ANY APPLICATION THAT IS DEVELOPED BY, PARTNERED WITH OR DEPENDENT ON A FOREIGN ENTITY IS NOT ELIGIBLE TO BE PART OF THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM.

E. THIS SECTION DOES NOT REQUIRE AN AGENCY TO CONNECT ANY SYSTEM TO THE INTERNET OR MAKE ANY SYSTEM CAPABLE OF RECEIVING INFORMATION FROM THE INTERNET. NOR DOES THIS SECTION AUTHORIZE ANY AGENCY TO IMPOSE SUCH REQUIREMENTS AS TO ANY OTHER GOVERNMENTAL DEVICE OR SYSTEM.

18-563. Auditor general; custodian; audits; findings

A. THE AUDITOR GENERAL IS DESIGNATED AS THE INDEPENDENT CUSTODIAN OF THE MASTER ENCRYPTION KEYS FOR THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM.

B. THE AUDITOR GENERAL SHALL DO ALL OF THE FOLLOWING:

1. ESTABLISH SECURE KEY MANAGEMENT, STORAGE AND ACCESS CONTROL PROCEDURES.

2. CONDUCT PERIODIC AUDITS OF ENCRYPTION COMPLIANCE AND INTEGRITY.

3. CERTIFY THE INSTALLATION AND OPERATIONAL VALIDATION FOR EACH STATE AGENCY THAT USES THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM.

4. REPORT ANY INSTANCE OF NONCOMPLIANCE TO THE GOVERNOR, LEGISLATURE AND ATTORNEY GENERAL.

C. ON THE REQUEST OF THE LEGISLATURE AND SUBJECT TO AVAILABLE MONIES, THE AUDITOR GENERAL SHALL CONDUCT A CYBERSECURITY AUDIT OF ANY STATE AGENCY THAT MAY INCLUDE ANY OF THE FOLLOWING:

1. VERIFICATION THAT THE STATE AGENCY'S STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM ENCRYPTION IS PROPERLY INSTALLED, CONFIGURED AND VALIDATED.

2. AN ASSESSMENT OF THE STATE AGENCY'S COMPLIANCE WITH CMMC 2.0 OR HIGHER CYBERSECURITY STANDARDS. THE ARIZONA DEPARTMENT OF HOMELAND SECURITY MAY BE ADVISED AND CONSULTED ON THE IMPLEMENTATION OF THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM BUT MAY NOT CHANGE PRODUCT OR INSTALLATION GUIDANCE.

3. A REVIEW OF THE STATE AGENCY'S ENCRYPTION KEY MANAGEMENT, ACCESS CONTROLS AND CUSTODY PROCEDURES.

4. AN EVALUATION OF THE STATE AGENCY'S ADHERENCE TO THE UNITED STATES DEPARTMENT OF DEFENSE RISK MANAGEMENT FRAMEWORK PRINCIPLES.

5. THE IDENTIFICATION OF ANY VULNERABILITIES, DEFICIENCIES OR NONCOMPLIANT PRACTICES.

6. RECOMMENDATIONS FOR CORRECTIVE ACTION AND A REMEDIATION TIMELINE.

D. THE AUDITOR GENERAL SHALL SUBMIT THE RESULTS OF AN AUDIT CONDUCTED PURSUANT TO SUBSECTION C OF THIS SECTION TO ALL OF THE FOLLOWING:

1. THE GOVERNOR.

2. THE LEGISLATURE.

3. THE PRESIDENT OF THE SENATE.

4. THE SPEAKER OF THE HOUSE OF REPRESENTATIVES.

5. THE CHAIRPERSONS OF THE SENATE AND HOUSE OF REPRESENTATIVES COMMITTEES WITH JURISDICTION OVER INFORMATION TECHNOLOGY ISSUES.

E. THE LEGISLATURE MAY USE THE AUDIT FINDINGS FOR ANY OF THE FOLLOWING PURPOSES:

1. LEGISLATIVE OVERSIGHT HEARINGS.

2. TO DETERMINE A STATE AGENCY'S APPROPRIATION.

3. CORRECTIVE ACTION DIRECTIVES.

4. ENFORCING COMPLIANCE WITH THE REQUIREMENTS PRESCRIBED IN THIS ARTICLE.

18-564. State agencies; vendors

A. A STATE AGENCY SHALL BE GIVEN THAT AGENCY'S KEY BUT MAY NOT RETAIN SOLE CUSTODY OR UNILATERAL CONTROL OF THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM ENCRYPTION KEYS.

B. EACH STATE AGENCY THAT USES THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM SHALL DO ALL OF THE FOLLOWING:

1. INSTALL THE STATEWIDE POST-QUANTUM CYBERSECURITY ENCRYPTION SYSTEM ON ALL OF THE STATE AGENCY'S SYSTEMS.

2. VALIDATE THE OPERATIONAL EFFECTIVENESS IN COORDINATION WITH THE AUDITOR GENERAL.

3. MAINTAIN CONTINUOUS COMPLIANCE WITH THE SYSTEM'S SECURITY REQUIREMENTS.

C. A STATE AGENCY'S INSTALLATION AND VALIDATION OF THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM MUST FOLLOW THE UNITED STATES DEPARTMENT OF DEFENSE RISK MANAGEMENT FRAMEWORK PRINCIPLES, INCLUDING CONTINUOUS MONITORING AND THREAT ASSESSMENTS.

D. ANY VENDOR THAT IS AWARDED A CONTRACT THAT WORKS WITH THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM SHALL DO ALL OF THE FOLLOWING:

1. PROVIDE TECHNICAL TRAINING AND OPERATIONAL SUPPORT TO THE AUDITOR GENERAL AND DESIGNATED STATE PERSONNEL.

2. SUPPORT THE INSTALLATION, VALIDATION AND AUDIT ACTIVITIES REQUIRED BY THIS SECTION.

3. PROVIDE DOCUMENTATION THAT DEMONSTRATES COMPLIANCE WITH CMMC 2.0 OR HIGHER STANDARDS.

4. COOPERATE FULLY WITH ALL STATE CYBERSECURITY AUDITS.

E. THE AUDITOR GENERAL MAY RECOMMEND SUSPENSION, REMEDIATION OR CONTRACT TERMINATION IF A VENDOR DOES NOT COMPLY WITH A REQUIREMENT FOR THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM.

F. A STATE AGENCY THAT DOES NOT COMPLY WITH A REQUIREMENT FOR THE STATEWIDE POST-QUANTUM CYBERSECURITY SYSTEM IS SUBJECT TO ALL OF THE FOLLOWING:

1. A MANDATORY CORRECTIVE ACTION PLAN IMPOSED BY JOINT RESOLUTION.

2. A LEGISLATIVE OVERSIGHT HEARING.

3. A RESTRICTION ON THE STATE AGENCY'S BUDGET THAT IS RELATED TO INFORMATION TECHNOLOGY EXPENDITURES.

G. THIS SECTION DOES NOT REQUIRE AN AGENCY TO CONNECT ANY SYSTEM TO THE INTERNET OR MAKE ANY SYSTEM CAPABLE OF RECEIVING INFORMATION FROM THE

INTERNET. NOR DOES THIS SECTION AUTHORIZE ANY AGENCY TO IMPOSE SUCH REQUIREMENTS AS TO ANY OTHER GOVERNMENTAL DEVICE OR SYSTEM.

Sec. 2. Legislative findings

The legislature finds:

1. Cybersecurity threats posed by nation-state adversaries, criminal organizations and nonstate actors constitute a clear and present risk to the confidentiality, integrity and availability of this state's data and critical systems.

2. Advances in quantum computing pose a threat to legacy cryptographic standards currently used to protect sensitive government information.

3. The United States department of defense has established cybersecurity maturity model certification (CMMC) 2.0 as a baseline for protecting controlled unclassified information (CUI) and defense-related systems.

4. Due to recent cyberattacks on state agencies, this state must proactively adopt post-quantum cryptographic protections that meet or exceed federal defense standards to ensure long-term security, continuity of government operations and public trust.

5. It is the policy of this state to do all of the following:

(a) Implement a statewide cybersecurity architecture using post-quantum encryption.

(b) Align state cybersecurity practices with the United States department of defense risk-management and certification standards.

(c) Ensure that encryption key custody and oversight for post-quantum cybersecurity systems in this state are independent, auditable and secure.

(d) Restrict procurement of cybersecurity systems to trusted United States-based companies.