

Cybersecurity Infrastructure Modernization and Protection

Description of issue and how recommending the agency's request furthers the agency's mandates

The Arizona Secretary of State's Office (the Office) administers and protects some of Arizona's most critical public infrastructure, including statewide election systems, voter registration, campaign finance reporting, business filing systems, and numerous public-facing online services relied upon daily by millions of Arizonans.

The cybersecurity environment facing election officials has changed dramatically over the past several years. Election systems remain designated as critical infrastructure and continue to be attractive targets for foreign adversaries, cybercriminal organizations, and other malicious actors seeking to disrupt government operations or undermine public confidence in elections.

In June 2025, the Office successfully detected, contained, and mitigated a foreign cyberattack targeting the candidate portal. Although no sensitive election infrastructure was compromised, the incident highlighted both the effectiveness of the Office's cybersecurity personnel and the continued risks associated with aging technology systems that support critical state operations.

Recognizing the heightened cybersecurity threats facing Arizona leading into the 2026 election cycle, both the executive and legislative branches provided important one-time investments to strengthen the state's cybersecurity posture. The Governor awarded \$452,000 in American Rescue Plan Act (ARPA) funding, and the Joint Legislative Budget Committee subsequently approved \$650,000 for enhanced cybersecurity monitoring and election security operations. These one-time appropriations enabled the Office to significantly strengthen its cyber defenses by expanding security monitoring, improving threat detection and response capabilities, enhancing vulnerability management, and increasing incident response readiness during one of the state's highest-risk election periods.

For nearly a decade, Arizona and other states benefited from technical assistance, cyber threat intelligence, incident response coordination, vulnerability assessments, and other election security services provided by the U.S. Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC). But beginning in 2025, those federal partnerships were significantly reduced, creating uncertainty of the availability of election cybersecurity services that states had relied upon in previous election cycles. In response, Secretary Fontes formally sought clarification from DHS regarding what election security

services would continue to be available to Arizona and how states should prepare for the 2026 election cycle. The Office also worked with Arizona's congressional delegation, the Arizona Department of Homeland Security, and the Arizona National Guard to identify alternative sources of assistance.

Since that time, officials from DHS and CISA have indicated their intent to rebuild relationships with state election officials and gradually restore portions of the federal election security partnership. Likewise, Arizona has continued participating in information-sharing programs through a subscription-based membership with the Multi-State Information Sharing and Analysis Center (MS-ISAC), which continues to provide valuable cyber threat intelligence, best practices, and technical guidance, albeit at a reduced level of service compared to previous years. These are positive developments, and the Office welcomes continued collaboration with its federal partners as those relationships evolve.

However, the scope, timing, and long-term availability of federal assistance remain uncertain. Regardless of how much federal cybersecurity support Arizona ultimately receives, it will not resolve the Office's most significant technology challenge: its reliance on obsolete infrastructure supporting elections, business services, campaign finance reporting, and public records.

Many mission-critical applications use outdated programming languages and decades-old architecture maintained by only a small number of current employees and retired contractors. Some have become single points of failure, increasing cybersecurity and operational risks, driving up maintenance costs, and limiting the Office's ability to meet evolving statutory and customer service needs.

Cybersecurity operations and technology modernization are complementary, but not interchangeable. Threat monitoring, vulnerability assessments, incident response, and intelligence sharing remain essential, but they cannot eliminate the risks created by obsolete applications. Arizona's most effective long-term strategy is to pair strong cybersecurity operations with modern, secure, and resilient technology infrastructure.

The Governor's and legislature's one-time cybersecurity appropriations successfully strengthened Arizona's operational defenses leading into the 2026 election cycle. This request builds upon those investments by addressing the underlying technology risks they were never intended to solve. Rather than funding temporary operational enhancements, this proposal completes the next phase of Arizona's enterprise technology modernization strategy by replacing aging infrastructure, modernizing mission-critical applications, expanding secure cloud-based services, reducing technical debt, and providing the personnel necessary to maintain Arizona's critical technology systems for years to come.

Completing this modernization effort will significantly improve the resilience, security, and reliability of the technology supporting Arizona's elections, business services, public records, and other statutory responsibilities while reducing long-term maintenance costs and strengthening Arizona's ability to defend its critical infrastructure against future cyber threats.

Proposal

Appropriate \$8,321,000 in one-time, nonlapsing funds from the state General Fund and seven (7) FTEs in FY2028, and \$2,626,000 annually beginning in FY2029, to complete modernization and secure Arizona's critical technology infrastructure.

The request consists of the following components:

Total Request

Initiative	FY2028 One-Time	FY2029+ Ongoing
Campaign Finance Platform Replacement	\$4,500,000	\$900,000
Enterprise IT and Security Modernization	\$2,750,000	\$655,000
Seven Information Technology FTEs	\$1,071,000	\$1,071,000
Total	\$8,321,000	\$2,626,000

The proposal includes:

- **Enterprise IT and Security Modernization:** The Office continues to rely upon multiple legacy applications developed over several decades to administer elections, manage business filings, and provide essential public services. Many of these applications utilize aging architecture that requires specialized knowledge possessed by only a handful of current employees and retired contractors. Continued reliance on these systems increases cybersecurity risk, operational complexity, and maintenance costs. Funding will support migration to secure, modern, low-code/cloud-based platforms while reducing technical debt and strengthening operational resilience.
- **Campaign Finance Platform Replacement:** Arizona's current campaign finance application and public-facing disclosure portal have exceeded their intended lifecycle and no longer meet modern expectations for security, reliability, transparency, or usability. Since submitting its FY2027 Executive Budget Request, the Office has conducted additional planning and technical evaluation of the

project, resulting in a more comprehensive understanding of the scope, complexity, and cost of replacing the existing platform.

The revised cost estimate reflects more than simply implementing a new Software-as-a-Service (SaaS) solution. It includes the complex migration of nearly three decades of campaign finance data dating back to 1996, accumulated across multiple technology platforms, software architectures, statutory changes, and successive Secretary of State administrations. Successfully replacing the current system will require extensive data discovery, cleansing, normalization, validation, and migration to ensure that historical campaign finance records remain complete, accurate, searchable, and publicly accessible throughout the transition. These data hygiene and conversion activities represent a significant portion of the overall project and are essential to preserving the integrity and continuity of Arizona's campaign finance records.

Funding will replace the existing campaign finance platform with a secure, commercial SaaS solution that improves cybersecurity, enhances public transparency, modernizes electronic filing and disclosure, simplifies long-term maintenance, and provides significantly improved services to candidates, committees, filing officers, journalists, researchers, and the public. The ongoing funding will support software licensing, cloud hosting, vendor maintenance, cybersecurity updates, and future statutory and operational enhancements.

- **Enterprise Cybersecurity Staffing:** Seven permanent information technology positions will provide the expertise necessary to design, implement, secure, maintain, and continuously improve Arizona's critical technology infrastructure. These positions ensure that modernization investments remain sustainable and reduce long-term dependence on external contractors.

Alternatives considered and reasons for rejection

The Office considered continuing its current approach of extending the useful life of legacy applications through incremental maintenance and targeted cybersecurity improvements. This alternative was rejected because it perpetuates increasing technical debt, maintains multiple single points of failure, and ultimately results in higher long-term costs.

The Office also considered delaying modernization until existing systems experience major operational failures. Given the mission-critical nature of these systems and the increasing sophistication of cyber threats targeting election infrastructure and state government, delaying modernization presents unacceptable operational, cybersecurity, and financial risk.

While prior appropriations have substantially strengthened Arizona's cybersecurity posture, they have primarily addressed security tools rather than the underlying legacy technology creating the greatest long-term risk. Completing enterprise modernization represents the most cost-effective and sustainable approach.

Impact of not funding this fiscal year

Failure to fund this request would significantly increase Arizona's long-term operational and cybersecurity risk by:

- Increasing exposure to sophisticated cyber threats targeting election and government infrastructure.
- Increasing the likelihood of service disruptions affecting voters, businesses, candidates, and government agencies.
- Continuing reliance on aging technology platforms that become increasingly expensive and difficult to maintain.
- Extending dependence on legacy applications supported by a limited number of technical personnel.
- Delaying replacement of systems that represent operational single points of failure.
- Increasing future modernization costs due to continued technical debt.
- Limiting the Office's ability to recruit and retain highly qualified information technology professionals.

Arizona has made significant progress strengthening its cybersecurity capabilities. This request represents the next and necessary phase of that effort by replacing the aging technology that continues to present the greatest operational and cybersecurity risk.

Statutory reference

A.R.S. §§ 16-142, 16-168, 41-151.12, 41-192, and other applicable statutes governing elections, information technology, cybersecurity, business services, and public records.

Equipment to be purchased

Enterprise software, cloud infrastructure, cybersecurity platforms, network equipment, application modernization tools, software licensing, and related information technology necessary to modernize and secure the Office's critical systems.

Classification of new positions

- **Principal IT Architect:** This position will be responsible for designing and identifying technical solutions for operational problems, including identifying best practices and implementing best-in-class architectural standards to any new solution. This is a senior technical role that can provide guidance across a multitude of applications as well as network, security, and infrastructure. **Senior IT Engineer:** This position will be responsible for maintaining network infrastructure, cloud configurations, firewall maintenance, and architecting new infrastructure solutions.
- **Senior Systems Engineer:** This position will be responsible for server maintenance and configuration and managing new software implementation in the server environment, including all Development-Security-Operations coordination.
- **Senior Security Analyst:** This position will be responsible for day-to-day security monitoring, threat analysis, and incident response, ensuring continuous threat detection and rapid response. This role will enable the senior security engineer to focus on higher-level architecture and long-term security improvements while maintaining a strong security posture across all systems.
- **Senior Developer (2):** These positions will be responsible for building and maintaining applications, including maintaining and creating new code as necessary in multiple system languages.
- **Quality Assurance (QA) Tester:** This position will be responsible for testing software solutions prior to deploying them to production, including creating and maintaining a QA center of excellence within the Office's IT department.

These positions are essential to completing enterprise modernization, maintaining secure operations, reducing reliance on external contractors, and ensuring long-term support for Arizona's critical technology infrastructure.

Annualization

\$2,626,000 in FY2029 and thereafter