Day Late and a Dollar Short

Historical Underfunding of Arizona's Elections and Federal Deprioritization of Elections and Elections Security

Executive Summary

Arizona administers one of the nation's most scrutinized election systems. Every election requires the coordination of thousands of election workers, hundreds of polling locations, dozens of interconnected technology platforms, thousands of pieces of election equipment, and a statewide voter registration system serving all 15 counties. Every voter registration transaction, candidate filing, campaign finance report, election-night result, and ballot status inquiry depends on technology that must operate securely, accurately, and without interruption.

Protecting that infrastructure has become increasingly difficult.

Since January 2023, the Arizona Secretary of State's Office (the Office) has repeatedly warned that many of the state's election technology systems are teetering on the edge of failure. Year after year, formal budget requests have identified aging software, increasing cybersecurity risks, growing maintenance costs, limited staffing, and the need to replace critical applications before they become nonoperational or security liabilities. Collectively, those requests sought more than **$17 million** in cybersecurity and information technology modernization funding from the state legislature.

Those warnings largely went unanswered.

While the legislature provided one-time appropriations for specific projects and temporary operational needs, the office has never received the sustained investment necessary to modernize its election technology infrastructure. Instead, election officials have relied on temporary appropriations, limited federal HAVA grants, expiring American Rescue Plan Act (ARPA) funding, interagency partnerships, and extraordinary efforts by existing staff to keep critical systems operating safely.

At the same time, the federal election security environment has changed dramatically under the second Trump administration to the detriment of election integrity nationwide.

For nearly a decade, the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) treated election infrastructure as part of the nation's critical infrastructure. States received cyber and election specific threat intelligence, vulnerability assessments, physical security reviews, tabletop exercises, incident response assistance, and coordination with federal intelligence and law enforcement agencies.

Beginning in early 2025, much of that support was suspended or indiscriminately cut while DHS reviewed CISA's election security mission. Election officials across the country—including Arizona—lost access to dedicated election security personnel, coordinated assessments, and federally supported information-sharing resources that had become integral components of their cybersecurity programs.

Arizona immediately sought clarification.

On March 7, 2025, Arizona Secretary of State Adrian Fontes wrote to federal officials requesting information about the future of federal election security assistance and warning that the withdrawal of CISA resources would leave states more vulnerable to increasingly sophisticated cyber threats. The letter emphasized that foreign adversaries, ransomware organizations, and politically motivated attackers would not pause their activities simply because federal support had been reduced. The Office requested guidance regarding what assistance would remain available and how states should prepare if longstanding federal partnerships were being dismantled.

No response was received.

Just months later, Arizona experienced exactly the type of incident the Office had warned about.

In June 2025, attackers believed to be affiliated with Iran compromised Arizona's online candidate portal, replacing candidate photographs with an image of Ayatollah Ruhollah Khomeini. Although the attack did not compromise voter registration information or election results, it demonstrated that Arizona's election infrastructure had become a target for hostile foreign actors seeking to undermine confidence in American elections.

Arizona successfully contained the incident.

Working with the Arizona Department of Homeland Security, the Arizona National Guard, the Arizona Counter Terrorism Information Center, county partners, and internal cybersecurity personnel, the Office isolated the intrusion, protected critical election systems, and restored operations without disruption to election administration. The Office ensured U.S. DHS was notified and shared threat intelligence with the community to ensure the attack here was not successful anywhere else. Sharing threat intelligence was politicized, which is a danger to all cybersecurity as it has a chilling effect on organizations sharing threat intelligence.

That success should not obscure our larger reality.

Arizona prevented a potentially significant cybersecurity incident despite years of structural underinvestment—not because the state's election infrastructure was adequately funded.

Rather than receiving sustained appropriations for modernization, the Office assembled a patchwork of temporary resources, one-time legislative appropriations, federal relief funding passed under President Biden, state partnerships, and operational efficiencies to prepare for the 2026 election. Those efforts deserve recognition. They also illustrate a troubling reality: Arizona has been forced to defend permanent critical infrastructure with temporary funding and the ingenuity of staffing resources already spread alarmingly thin

Compounding these operational challenges, Arizona also faced an unprecedented series of federal legal and policy disputes concerning election administration. Between 2025 and 2026, the state defended itself against federal litigation seeking confidential voter registration information, responded to executive orders attacking election administration, addressed demands for expanded voter data, and navigated a rapidly evolving federal policy environment. Throughout these disputes, the Office continued administering elections while simultaneously defending Arizona's authority to manage elections in accordance with state and federal law.

Against that backdrop, DHS Secretary Markwayne Mullin announced in July 2026 that CISA resources would again be made available to assist states before the general election.

Arizona welcomes that announcement but will not be caught holding its breath.

Election security should never be partisan. Foreign adversaries do not distinguish between Republican and Democratic election officials. Every successful cyberattack against election infrastructure weakens confidence in American democracy regardless of political outcome. State and federal governments should work together whenever possible to defend election systems against common threats.

But rebuilding that partnership requires more than empty promises.

It requires restoring trust, rebuilding professional relationships, providing predictable technical assistance, and investing in the infrastructure that election officials have warned for years must be replaced.

This report argues that Arizona's experience demonstrates three fundamental lessons.

First, election cybersecurity is no longer simply an information technology issue. It is a matter of homeland security and critical infrastructure protection. The federal government has removed themselves from the equation of support historically relied upon by election administrators and have taken an adversarial position against states as the 2026 general election inches closer.

Second, temporary funding cannot substitute for long-term modernization. Monitoring aging systems does not replace them. Emergency appropriations do not eliminate technical debt. Dedicated public servants cannot indefinitely compensate for obsolete technology.

Third, Arizona has demonstrated responsible stewardship despite limited resources and a growing threat landscape. The Office identified risks before they became crises, requested funding through established budget processes, strengthened partnerships with state agencies, defended election systems against foreign cyber activity, protected voter privacy, and continued modernizing wherever resources permitted.

The challenge Arizona faces today is therefore not one of commitment or competence.

It is one of capacity.

To address that challenge, this report recommends two immediate actions:

- **An immediate $2 million federal election security partnership** to support cyber monitoring, incident response, vulnerability assessments, county security assistance, and election readiness activities before the 2026 General Election.
- **A three-year, $30 million state-federal modernization partnership**, including:
    - **$20 million** to replace Arizona's statewide voter registration system and related county integrations; and
    - **$10 million** to modernize election technology infrastructure and establish sustainable cybersecurity capabilities.

The purpose of these recommendations is not simply to improve Arizona's election administration–it is to protect critical infrastructure that serves every Arizona voter and contributes to the security of American democracy.

Introduction

Election Security Is National Security

The integrity of an election depends on far more than ballots and voting machines.

Modern elections rely on an interconnected ecosystem of technology that begins long before Election Day and continues long after the final ballot is counted. Voter registration databases verify eligibility. Candidate filing systems determine who appears on the ballot. Campaign finance platforms promote transparency. Election management systems prepare ballots, and coordinate county operations. Election Night Reporting systems provide timely unofficial results. Public websites deliver trusted information to millions of voters. Every component must function accurately, securely, and continuously.

Collectively, these systems constitute critical infrastructure.

Arizona's election system is particularly complex because elections are administered through a decentralized partnership involving the Secretary of State and fifteen independently operated counties. Thirteen counties rely directly on the statewide Access Voter Information Database (AVID) as their primary voter registration system. The remaining two counties maintain local registration systems but still depend upon AVID for statewide voter registration coordination, duplicate record management, voter history, federal reporting, and statewide election administration.

This decentralized model has many strengths. Local election officials understand their communities, maintain close relationships with voters, and administer elections that reflect local needs while operating within a consistent statewide legal framework.

It also creates cybersecurity challenges.

Each county operates different technology environments, employs varying levels of information technology staff, contracts with different vendors, and manages unique operational risks. Large urban counties may maintain dedicated cybersecurity personnel and sophisticated information technology departments. Smaller rural counties often depend more heavily on state assistance, regional partnerships, and federal expertise.

Because these systems exchange information continuously, cybersecurity is only as strong as the weakest connection.

A vulnerability affecting a vendor, a county network, or a statewide application can have consequences that extend well beyond a single jurisdiction. Likewise, a successful attack against a public-facing system may not compromise election results but can still erode public confidence, disrupt operations, require expensive emergency responses, and consume desperately needed resources.

Recognizing these realities, the federal government designated election infrastructure as critical infrastructure in 2017 and developed extensive partnerships between Cybersecurity and Infrastructure Security Agency (CISA) and state election officials. Those partnerships reflected an important principle: while states administer elections, as outlined in the Constitution, defending election infrastructure against sophisticated nation-state cyber threats requires cooperation across all levels of government.

That principle remains true today.

Unfortunately, Arizona's ability to modernize its election infrastructure has not kept pace with the evolving threat environment.

For the entirety of this administration, the Secretary of State's Office (the Office) has warned that maintaining secure elections requires more than dedicated public servants and temporary appropriations. It requires sustained investment in technology, permanent cybersecurity capabilities, predictable partnerships, and long-term planning.

Those warnings became increasingly urgent as foreign cyber activity intensified, ransomware attacks targeted public institutions, artificial intelligence accelerated disinformation campaigns, and hostile governments demonstrated growing interest in election infrastructure.

Yet the state's modernization efforts continued to rely largely on one-time funding, temporary federal grants, and extraordinary efforts by existing personnel.

This report examines how Arizona arrived at that point.

It documents the repeated warnings issued by the Office, the funding requests submitted to state policymakers, the backsliding role of federal election security assistance, the operational challenges faced by Arizona election officials, and the steps taken to protect election infrastructure despite limited resources.

The report also considers what lessons Arizona's experience offers for the future.

Its central conclusion is straightforward.

Arizona's election officials have consistently demonstrated the professionalism, expertise, and commitment necessary to protect one of the United States' most visible election systems. What they have not received is a level of investment, by state or federal partners, commensurate with the importance of the mission they have been asked to perform.

Election security cannot depend indefinitely on temporary appropriations, aging technology, and the extraordinary dedication of public servants.

Protecting one of America's most important democratic institutions requires something more durable: bipartisan prioritization, sustained investment, modern infrastructure, and a renewed partnership among state and federal governments dedicated to securing elections against the threats of tomorrow.

I. Arizona Repeatedly Warned That Its Election Systems Required Modernization

Arizona's election infrastructure is not a single machine, website, or database. It is a complex, statewide technology ecosystem supporting every stage of the election process—from voter registration and candidate filings to ballot preparation, election administration, election night reporting, campaign finance disclosure, and post-election recordkeeping.

This infrastructure includes AVID, candidate filing applications, campaign finance reporting systems, election management software, election night reporting platforms, petition processing systems, county interfaces, cybersecurity tools, cloud services, databases, and numerous internally developed applications. These systems exchange information continuously among the Office, Arizona's 15 counties, appropriate state agencies, federal partners, vendors, and the public.

Arizona's decentralized election model is one of its greatest strengths, but it also presents unique cybersecurity challenges. While the Secretary of State maintains statewide systems and coordinates election administration, elections are conducted by 15 independently operated counties with varying technology environments, staffing levels, vendors, and cybersecurity capabilities. Larger counties often have the resources necessary to maintain dedicated information technology and cybersecurity staff, while many rural counties rely more heavily on state assistance and shared resources. Because these systems are interconnected, the security of Arizona's elections depends upon the resilience of the entire statewide network rather than any single system or agency.

Many of Arizona's election systems were developed years—or in some cases decades—apart using different technologies and architectural approaches. Several continue to rely on custom-built applications, fragmented databases, aging software, limited vendor support, or specialized institutional knowledge possessed by only a handful of employees or contractors. The Office's FY2027 budget request described portions of this environment as relying on "fragile, decades-old, in-house code," with some critical systems supported by a single contractor.

These conditions create operational, financial, and cybersecurity risks that grow more significant each year. Aging technology becomes more expensive to maintain, more difficult to secure, and increasingly incompatible with modern cybersecurity standards. Delaying replacement does not eliminate these costs, it generally increases them while also expanding the state's exposure to avoidable risk.

Recognizing these challenges, the Office repeatedly warned state policymakers that Arizona's election technology required sustained investment. Beginning in January 2023, successive budget requests documented increasing cybersecurity threats, aging infrastructure, staffing

shortages, technical debt, and the need to replace critical systems before they became operational or security liabilities.

State Funding Requests

The publicly available record reflects a consistent pattern of identifying technology risks and requesting resources to address them.

Fiscal Year	Documented Request or Warning	Legislative Response
FY2024	Requested funding for 11 additional positions, including Arizona's first Chief Information Security Officer and six positions supporting county election administration and statewide election operations.	Provided a limited, temporary appropriation sufficient to support approximately two of the requested positions through the administration's term.
FY2025	Renewed requests for election administration, legal services, records management, staffing, technology modernization, and operational support.	Several needs remained unresolved, and the Office continued relying on temporary appropriations, grants, and operational efficiencies.
FY2026	Following the foreign cyberattack on Arizona's candidate portal, requested approximately **$10 million** in immediate modernization funding and **$3.5 million annually** for ongoing cybersecurity operations and system maintenance.	No comparable permanent cybersecurity modernization appropriation was enacted.
FY2027	Submitted a comprehensive cybersecurity modernization proposal requesting **$9.421 million** in one-time funding, seven permanent cybersecurity positions, and **$3.771 million** in annual operating support.	As of this report, the comprehensive modernization proposal had not been funded.

Taken together, the Office's budget requests demonstrate a consistent effort to sound the alarm about emerging risks before they materialize into operational crises. Since January 2023, the Office has formally requested more than **$17 million** in cybersecurity and information technology modernization funding.

The legislature has provided important one-time appropriations and project-specific investments that helped maintain operations and address a few immediate priorities identified by the Office. Those investments have been valuable and have produced measurable improvements. However, they have not established a permanent funding structure capable of replacing

Arizona's aging election technology, sustaining a dedicated cybersecurity operation, or modernizing the interconnected systems that support statewide election administration.

The FY2027 cybersecurity proposal illustrates the scope of those modernization needs. Rather than requesting discretionary technology upgrades, the proposal focused on replacing or securing systems that perform constitutionally and statutorily required election functions. The proposal included:

- **$2.5 million** to replace Arizona's campaign finance reporting platform, with **$750,000 annually** for ongoing operations and maintenance.
- **$3 million** to modernize election management systems, Election Night Reporting, the Candidate Portal, and E-Qual, with **$750,000 annually** for continuing support.
- **$350,000** for cloud migration and modernization of critical infrastructure, with **$200,000 annually** for hosting and operations.
- **$2.5 million** for broader information technology and cybersecurity modernization, including replacement of aging infrastructure, with **$1 million annually** for ongoing support.
- **$1.071 million** to establish seven permanent cybersecurity and information technology positions needed to operate and secure these systems.

In total, the proposal requested **$9.421 million** in one-time modernization funding and **$3.771 million** in recurring annual support.

To be clear, these requests were not intended to expand government services or introduce optional technology enhancements. They were designed to replace aging systems that support core election functions required by Arizona law, reduce long-term maintenance costs, improve cybersecurity resilience, strengthen continuity of operations, and ensure that Arizona's election infrastructure remains reliable in an increasingly complex threat environment.

The underlying urgency is driven by structural deficiencies rather than temporary inconvenience. Election technology cannot be modernized through periodic emergency appropriations alone. Major system replacements require years of planning, procurement, software development, county integration, data conversion, testing, security validation, and training. Delaying investment does not simply postpone spending—it often extends reliance on increasingly obsolete technology, raises long-term maintenance costs, and narrows the window available to complete critical projects before future election cycles.

II. Federal Election-Security Assistance Was Dismantled

CISA’s election-security work grew out of the federal designation of election systems as critical infrastructure. Before 2025, CISA and its partners provided states with services that included:

- election-specific threat intelligence;
- vulnerability scanning and cyber assessments;
- physical-security inspections;

- tabletop exercises and incident planning;
- coordination among state, local and federal agencies;
- technical assistance during active incidents; and
- the EI-ISAC information-sharing network.

Arizona relied on these services. During the 2024 election, CISA helped coordinate threat information when polling locations received bomb threats and had previously assisted Arizona with preparedness exercises and physical-security reviews.

That support changed abruptly in 2025.

In February 2025, the U.S. Department of Homeland Security (DHS) paused CISA's election-security activities and announced a review of election-related personnel, programs, products, and funding. CISA also terminated federally funded support for the EI-ISAC, which had provided state and local election officials with cybersecurity monitoring and threat-sharing services.

By March 2025, election officials were reporting that CISA had halted the cyber and physical-security assistance on which states had relied.

Arizona asked for answers.

Arizona Secretary of State Adrian Fontes sent CISA and DHS correspondence dated March 7, 2025, and February 5, 2026, seeking information about federal election-security assistance. In a February 25, 2026, public statement, Secretary Fontes said DHS had not responded and urged the department to begin by answering those letters.

The loss was not merely financial. It weakened the trusted relationships necessary to exchange sensitive information quickly. By January 2026, election officials nationally were warning that trust between states and CISA had been damaged and might be difficult to rebuild.

III. Arizona Contained a Suspected Iranian Cyberattack Without Meaningful CISA Assistance

On June 23, 2025, hackers penetrated Arizona's online candidate portal. The attackers replaced candidate photographs with an image of Ayatollah Ruhollah Khomeini. Security officials later said they were moderately confident that the attack originated with Iran or Iranian-affiliated actors.

The incident did not compromise voter-registration information, ballot tabulation systems, or the ability to conduct an election. The Office detected the activity, contained the breach, removed the affected portal from service, and worked to restore it safely.

The response involved the Arizona Department of Homeland Security, the Arizona National Guard, the Arizona Counter Terrorism Information Center, and other state and law-enforcement partners.

Historically, an incident involving a suspected foreign government targeting election infrastructure would have triggered close coordination with CISA. But by June 2025, the federal partnership had been decimated by program cuts, staffing changes, politicization, and deteriorating trust.

Arizona succeeded because state employees and partner agencies acted quickly, not because the state had received the permanent funding or federal support it had requested.

Despite inadequately funded systems, dedicated public employees prevented an aging system from becoming a larger national-security incident.

That is not a sustainable security strategy.

IV. Arizona Cobbled Together Temporary Resources for 2026

With neither a comprehensive state appropriation nor dependable federal election-security assistance, the Office pursued every available alternative.

JLBC Election-Readiness Funding

The Office requested authority to redirect unspent funding from the 2025 Congressional District 7 special election toward statewide 2026 election readiness.

In early 2026, the Joint Legislative Budget Committee (JLBC) approved a $650,000 transfer for temporary cybersecurity monitoring and active cybersecurity management. The Office also requested approval for an additional $2.85 million for county voter services, BallotTrax and electronic ballot-curing tools, statewide voter-registration expenses, operational support, and other election-readiness needs.

The critical limitation is contained in the description itself: temporary cybersecurity monitoring.

Temporary monitoring may protect the election environment for a limited period. It does not replace aging applications, eliminate single points of failure, retain permanent personnel, or provide continuous protection between election cycles.

Governor’s ARPA Support

The Office also relied on federal American Rescue Plan Act (ARPA) resources made available through the Arizona Governor’s Office. ARPA funded election preparedness, county assistance, security activities, voter services, and other temporary initiatives.

These funds have produced measurable benefits, but ARPA is an expiring pandemic-relief program, not a permanent election-security funding source.

Arizona has therefore been forced to defend permanent critical infrastructure with temporary money.

V. The Federal Government Withdrew Assistance and Then Targeted Arizona’s Election Administration

The loss of CISA support did not occur in isolation. It coincided with a sustained federal campaign to illegally obtain private sensitive voter data, impose federal requirements on state election administration, erroneously investigate election officials, and challenge Arizona's authority in court.

March 25, 2025: First Federal Election Executive Order

On March 25, 2025, President Trump signed an executive order titled *Preserving and Protecting the Integrity of American Elections*. In total the Order's aim was to illegally and erroneously overhaul the nation's election system. It sought to impose federal proof-of-citizenship requirements, direct federal agencies to obtain and review state voter data, and change rules affecting ballot deadlines and election administration. The President claimed unilateral authority over election regulation violating the Constitution's clear distribution of power to the states over election administration.

The order was immediately challenged as exceeding presidential authority over elections, a power assigned principally to the states and Congress.

July 2025: DOJ Demands Arizona's Voter Registration Data

The U.S. Department of Justice (DOJ) illegally requested Arizona's unredacted statewide voter-registration database, without justification for the Department's intended use.

The requested records included sensitive data such as dates of birth, addresses, driver's license information, and portions of Social Security numbers. Arizona refused to provide an unredacted database, citing state and federal law.

January 6, 2026: DOJ Sues Arizona

On January 6, 2026, the DOJ, altering the office by tweet, sued Secretary Fontes to compel production of Arizona's detailed voter records.

The federal government argued that the Civil Rights Act justified the demand. Arizona argued that the statute did not entitle the DOJ to the unredacted database and that releasing the records would jeopardize voter privacy.

April 28, 2026: Arizona Wins the Voter-Roll Case

On April 28, 2026, U.S. District Judge Susan Brnovich dismissed the case with prejudice stating, "Accordingly, the Court will dismiss the Attorney General's claim with prejudice because amendment would be legally futile." The court concluded that Arizona's statewide voter-registration database was not a document the DOJ could demand under the law it had invoked.

The ruling was one of 21 of federal court decisions rejecting similar DOJ demands directed at other states.

March 31, 2026: Second Federal Election Executive Order

On March 31, 2026, President Trump issued another illegal executive order directing the development of federal voter-eligibility lists and instructing the U.S. Postal Service to limit the transmission of mail ballots based on those lists. During his press conference, the President threatened criminal penalties for election officials, mail carriers, and others who would send ballots to or deliver ballots from individuals the administration deems ineligible. A concrete move in the President's larger plans to pick his own acceptable list of voters.

The order raised immediate constitutional and operational concerns, particularly in states such as Arizona where more than 80% of voters routinely use early voting by mail.

June 25, 2026: Arizona Prevails in the Executive-Order Litigation

On June 25, 2026, Arizona Attorney General Kris Mayes announced a court ruling blocking the administration from implementing key portions of the March 31 order. The Attorney General characterized the order as an unlawful attempt to exert federal control over state elections.

The administration subsequently sought U.S. Supreme Court review of litigation involving the order.

July 2026: Escalating Federal Pressure

During July 2026, public statements and federal communications intensified concerns among state election officials regarding:

- federal election observers;
- possible investigations or prosecutions of election officials;
- demands concerning noncitizen registration and list maintenance;
- expanded federal access to state election information; and
- the administration’s effort to defend its election executive orders before the Supreme Court.

The Office submitted a Freedom of Information Act request seeking information about federal plans to deploy election observers in Arizona.

Several events contained in the Office’s working timeline—including particular calls, letters, observer discussions, and press-conference statements—should be supported with the underlying correspondence, transcripts, recordings, or federal notices before inclusion in an externally released version of this report.

VI. Now DHS and CISA Say They Want to Help

On July 17, 2026, DHS Secretary Markwayne Mullin delivered remarks concerning the administration’s election-integrity program and the federal government’s relationship with states. DHS indicated that CISA resources could again be made available to support state election security.

Secretary Mullin demanded states run their voter rolls through a federally controlled database maintained by DHS to determine if noncitizens were on lists. The Secretary provided no proof to

justify his claims but went so far as to threaten loss of federal grant access if states refused to comply.

Any restoration of legitimate cybersecurity and physical-security support is welcome. Foreign adversaries do not care whether the governor, secretary of state, president, or DHS secretary is a Democrat or Republican. They seek vulnerabilities, disruption, confusion, and loss of public confidence.

But the chronology matters.

Federal support was undermined at the direction of the White House and quickly withdrew rapidly in early 2025. Election-security organizations lost funding. Arizona's letters went unanswered. A suspected Iranian actor attacked an Arizona election portal. The federal government demanded confidential voter data, sued the state, pursued executive orders affecting state election administration, and threatened election officials with additional federal intervention.

Only after these events—and only weeks before the 2026 general-election period reached its most critical phase—did DHS publicly renew its offer of assistance.

That is the definition of a day late and a dollar short.

Moreover, statements of support are not the same as operational capacity. Arizona needs clear answers:

1. Which CISA services are immediately available?
2. Which experienced personnel will be assigned to Arizona?
3. Will CISA restore real-time election threat intelligence?
4. Will it conduct cyber and physical-security assessments?
5. Will it support incident response during the general election?
6. Will services be available to Arizona's 15 counties?
7. What information will CISA require from the state?
8. How will sensitive state information be protected from political misuse?
9. Are services conditioned on compliance with unrelated federal election-policy demands?
10. What funding will accompany the assistance?

Trust cannot be restored through a press conference alone. It must be rebuilt through resources, professional conduct, clear safeguards, and sustained cooperation.

VII. What Meaningful Federal Assistance Should Look Like

Arizona should accept federal assistance that is lawful, professional, technically useful, and protected from partisan misuse. But assistance must be proportional to the risk and must address both the immediate election and the structural weaknesses that produced the current crisis.

1. Provide $2 Million Immediately for the 2026 Election

DHS and CISA should provide Arizona with at least $2 million in immediately deployable election-security assistance.

The funding should support:

- continuous network and endpoint monitoring through certification;
- surge incident-response capacity;
- county vulnerability assessments;
- physical-security reviews;
- penetration testing and remediation;
- threat-intelligence services;
- tabletop exercises and continuity planning;
- backup communications systems;
- security support for county election offices;
- emergency vendor assistance; and
- post-election monitoring through canvass and certification.

The resources should be provided without conditioning cybersecurity assistance on the surrender of confidential voter data or acceptance of disputed federal election policies.

2. Establish a $30 Million, Three-Year Modernization Partnership

Immediate security monitoring cannot repair obsolete infrastructure. DHS, CISA, and Congress should therefore establish a three-year, $30 million modernization partnership with Arizona.

$20 Million: Statewide Voter Registration Modernization

AVID is the statewide voter-registration system required to coordinate registration records and election functions across all 15 counties.

Thirteen counties rely on AVID as their principal voter-registration platform. The two remaining counties use separate county systems but still depend on AVID for statewide data exchanges, duplicate-registration review, federal reporting, voter history, list maintenance, and other statewide functions.

The replacement project should include:

- procurement and development of a modern statewide registration platform;
- data cleansing and migration;
- county-system integrations;
- identity, eligibility, and citizenship-verification interfaces;
- military and overseas-voter functions;
- list-maintenance tools;
- disaster recovery and redundant hosting;
- security testing;
- accessibility;
- training;
- parallel operations and acceptance testing; and

- ongoing maintenance during implementation.

The Office's current estimate is approximately $15 million for the core replacement project. A $20 million federal commitment would provide an appropriate contingency for data conversion, county interfaces, independent security testing, federal integrations, inflation, and transition support.

$10 Million: Election IT and Cybersecurity Modernization

An additional $10 million should modernize the election applications and security environment surrounding the voter-registration system.

Priority projects include:

- candidate-filing and petition systems;
- election-management applications;
- campaign-finance reporting;
- cloud migration;
- identity and access management;
- network segmentation;
- security logging and event management;
- endpoint detection and response;
- backup and recovery;
- secure software development;
- vendor-risk management;
- vulnerability remediation;
- permanent cybersecurity personnel; and
- a statewide election-security coordination capability serving counties.

This investment closely reflects the modernization needs Arizona has already documented in its state budget requests.

VIII. Conclusion

Arizona's election officials have done what taxpayers should expect of them.

They identified risks before a crisis occurred. They presented detailed funding requests. They established a chief information security officer and an election cybersecurity unit. They worked with state partners, counties, the governor, the legislature, the Arizona National Guard, and outside experts. They detected, contained, and verified no sensitive information was accessed or even attempted to be accessed, they then remediated and hardened systems against further attack and shared this threat intelligence immediately so election systems could be protected nationwide against this adversary. They protected voters' private information in federal court. And they assembled temporary resources to prepare for the 2026 election.

What they have not received is the stable investment necessary to protect one of the nation's most closely watched election systems.

For years, Arizona was told to do more with less. When federal support disappeared, the state did more with almost nothing. When the systems were attacked, Arizona stopped the attack. When federal agencies demanded confidential voter information, Arizona defended its voters and prevailed.

Now the federal government says it wants to help.

Arizona will gladly accept real help—but unless that help is immediate, substantial, professional, unconditional, and sustained, it will amount to nothing more than another election-related headline-seeking claim.

Because a temporary offer weeks before an election is not a cybersecurity strategy.

We all know, a press conference is not an appropriation.

And after years of warnings, an international cyberattack, unanswered letters, temporary patches, and repeated litigation, another promise without resources would be exactly what Arizona has received for too long:

A day late and a dollar short.

Appendix A: Verified Public Timeline

Date	Event
January 20, 2025	New presidential administration begins.
February 2025	DHS pauses CISA election-security work and ends federal support for EI-ISAC activities.
March 7, 2025	Arizona Secretary of State sends correspondence to the DHS Secretary seeking information about CISA support.
March 25, 2025	President signs executive order concerning federal election policy, citizenship documentation, voter records, and ballot rules.
June 23, 2025	Suspected Iranian-linked attackers penetrate Arizona's candidate portal.
July 28, 2025	DOJ requests Arizona's detailed statewide voter-registration records.
August 12, 2025	Secretary Fontes publicly requests approximately $10 million immediately and $3.5 million annually for cybersecurity modernization.
September 2025	SOS submits FY2027 proposal including $9.421 million for modernization and $3.771 million annually.

January 6, 2026	DOJ sues Arizona to obtain statewide voter-registration data.
January 29, 2026	JLBC considers and approves $650,000 for temporary cybersecurity monitoring.
February 5, 2026	SOS sends additional correspondence concerning DHS and CISA support.
February 25, 2026	Secretary Fontes publicly calls on DHS to answer the March 2025 and February 2026 letters.
March 31, 2026	President issues executive order involving federal voter-eligibility lists and mail-ballot transmission.
April 28, 2026	Federal court dismisses DOJ's Arizona voter-data lawsuit with prejudice.
June 25, 2026	Court blocks significant portions of the March 31 election executive order.
July 17, 2026	DHS Secretary Mullin delivers remarks on federal election-integrity efforts and renewed support for states.
July 24, 2026	SOS reports that more than $4.22 million has been made available to counties since 2024 through ARPA and JLBC-supported resources.