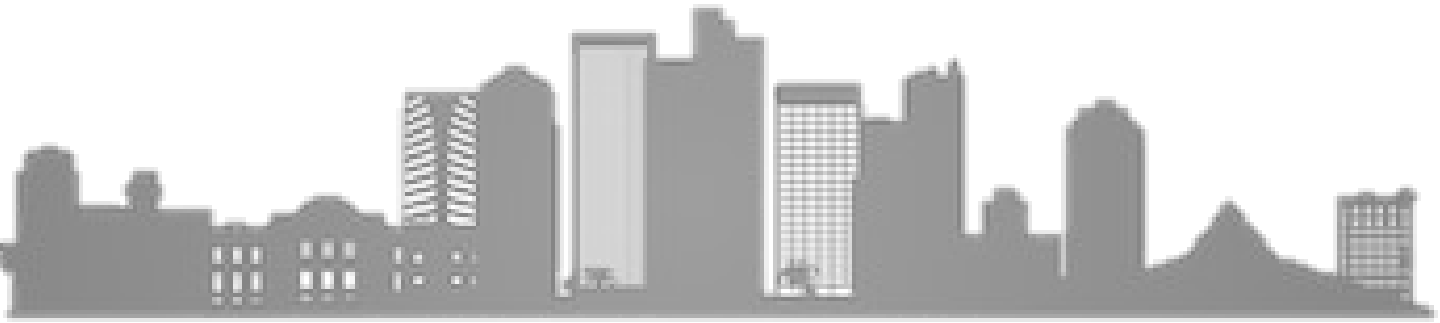
Arizona Secretary of State
Elections Security Report

Prepared for the
Arizona Department of State

by Gartner

Table of Contents



A Message from the Secretary

"Election security and integrity have been the top priority for my administration. Arizona needs to be able to trust the outcome of our elections. The fundamental philosophy of my office is that it should be easy to vote and hard to cheat. Cybersecurity is a race without a finish line and that is why, over the years, we have made many upgrades enhancing the security of both our election systems and the security of your personal information.

We live in a connected, albeit wireless, world. It's a world of great convenience but each new convenience creates new security risks and vulnerabilities. Arizona has utilized a portion of the new funding issued by the Election Assistance Commission's Help America Vote Act Security Fund to undertake a comprehensive, industry standard evaluation of our entire IT network. Given that we are only as strong as our weakest link..

Michele Reagan

Secretary of State
State of Arizona

Election security, regardless of the medium, is a culture that needs to be championed from the highest election official to the newest poll worker. The Secretary of State's Office will continue to work closely with the fifteen counties of Arizona to help foster that culture of security. The human element is the largest unknown factor in any cybersecurity plan and providing ongoing training and forums for information sharing is a long-term goal.

Let me be clear – previous attacks have failed but as sophisticated hackers around the globe continue to look for ways into our systems, we must continue to invest in security and work wit hour county and federal partners to prevent any issues before it is too late.

Executive Summary

Two years after the first known attempts to access voter registration rolls were discovered, the United States as a whole has made investments into improving the integrity of the election process. While Arizona is capitalizing on the federally-driven improvements in election-related intelligence, the Arizona Secretary of State wanted to ensure that a comprehensive plan was in place to address all known security vulnerabilities, protect the voter's personal information that was the target of the last attempt, and ensure the integrity of the election process.

In order to mitigate risks and vulnerabilities, the Arizona Secretary of State contracted with Gartner, Inc. to assess the level of security maturity through an extensive review of the Arizona Secretary of State's information security policies, procedures, and technologies related to elections security. The in-depth analysis led to the identification of gaps against the desired state. This review was backed by targeted threat-based intelligence testing using the same approaches taken by bad actors. From these efforts, a comprehensive set of recommendations and a prioritized, phased roadmap was developed and aligned with the risk mitigations required to improve the election's security posture.

While significant progress has already been made – in part due to the injections of Help America Vote Act Security Fund –and improvements in statewide security efforts, there is still work to do. However, with clearly identified objectives and actions, improvements in the security posture at the Arizona Secretary of State will have far-reaching impacts in the protection of the voters, election systems, and the integrity of the democratic systems.

Key Recommendations

- Strengthen and formalize processes, documentation and standards to facilitate comprehensive management, maintenance and use of current-state technology
- Foster a culture of security to enable cost-effective protections commensurate with the risk and value of critical and sensitive software, hardware, and information
- Enhance strategies for the use of user identities, mobile devices, and transaction monitoring information to improve the effectiveness of existing security controls

The National Elections Posture

Following Russian interference in the 2014 Ukrainian presidential election, the United States was on high-alert when attempts to access voter registration systems in 2016 were first discovered. Two years into the investigations of those attempts, it is now known that at least 21 states are known to have been targeted. While a small number of jurisdictions confirmed attempted compromises of telecommunications networks supporting various election processes, only Illinois confirmed hackers had succeeded in breaching its voter systems while California vehemently denied the reports of any compromise at all.

In addition to coordinating investigations related to the source of the attacks by the Federal Bureau of Investigation and the Department of Homeland Security, the federal government also responded by including the Help America Vote Act (HAVA) Election Security Fund as part of the Consolidated Appropriations Act of 2018, signed by the President in March 2018. The Fund is intended to provide states with the additional resources necessary to enhance the protection and overall security of their election systems.

The investigations have revealed widespread use of social media in organized campaigns of disinformation, as well as the attempt to compromise voter registration information systems by nation-state and criminal actors. While it is interesting to note that no evidence has surfaced related to alterations of actual exercised votes, many agree that the multiple attempted compromises were intended to cause chaos and confusion, with the hopes of causing general citizen mistrust of the election process. For example, there are indicators that in some cases, voter registration data was modified to reflect incorrect eligibility to vote or altered voting locations.

A Multi-Pronged Approach to Data Collection

1. Spearfished a U.S. election software company based in Florida, as well as targeted democrats and targeted republicans (2015)
2. Compromised Democratic Congressional Campaign Committee and Democratic National Convention computers (2016)
3. Researched web addresses used by U.S. state board of elections, secretaries of state, and other election related entities for website vulnerabilities (2016)
4. Attempted Access of Voter Registration Systems in 21 states (2016)

Election system security enhancements are badly needed with national election automation infrastructure continuing to be rolled out without necessary security planning, at least to this point. With the vast expansion in the use of technology to improve voter convenience and reduce government costs, most election administration officials, from Lt. Governor to the Secretary of State to County Clerk, come into office without realizing the need for them to also take on the role of IT Director for election systems within their jurisdictions.

As is true in most instances of modernization and automation, manual processes simply do not translate directly to the use of technology. Automating inefficient or weak manual processes simply enables the execution of bad processes faster. Without appropriate leadership and oversight, technology is often deployed that lacks basic protection controls, is exposed to basic electronic compromise, and election processes lack comprehensiveness resulting in an insufficient ability to maintain the integrity of citizen data and votes.

"The prospect of a hostile government actively seeking to undermine our free and fair elections represents one of the gravest threats to our democracy since the Cold War,"

Senate Minority Leader Harry Reid, D-Nev., in a letter to the FBI

Challenges in Arizona

The importance of administering secure elections cannot be overstated…

…in Arizona or in any other state. Current geopolitical events in cyberspace affecting elections across the United States since 2016 have increased scrutiny on the systems and processes that support the elections. In particular, Arizona citizens want to know that elections are secure and that action is being taken to reinforce the elections process. The fundamental philosophy is that voting should be easy and interfering with the election should be difficult.

The confirmed June 2016 attempted access of the Arizona voter registration system via successful phishing of a county election official led to public scrutiny in the State and across the nation.

While no voter data was compromised, altered, or stolen, it is clear that election data is and will remain an important and viable target for misappropriation for the foreseeable future.

This is reflected in the Department of Homeland Security's designation of elections systems now being part of the nation's critical infrastructure in 2017.

However, compromising a well-protected technology infrastructure is difficult and costly. Similarly, building a well-protected technology infrastructure is also difficult and expensive, but it is achievable with appropriate funding and resources. And once achieved, a well-protected technological approach may tend to drive attackers to pursue other, less-protected sources and seek valuable information elsewhere. However, well-protected technology is not the only answer. In fact, while important and necessary, well protected technology is not the only factor in a secure election system.

The cyber-security industry recognizes that the overwhelming majority of technology compromises and information exposures have a root-cause based in **failures of process, people, and awareness**. Such failures are many times driven by policies and processes that are missing, incomplete, unenforced, or not applied comprehensively. Unfortunately, to have good processes and policies requires people to build them. Thus, insufficient numbers of skilled people, or people without adequate training, only make the challenges of protecting information greater.

Technology-based election systems that are typically under-staffed and overworked, or personnel who are not properly trained and experienced, will generally, without fail, result in processing or configuration errors and oversights that over time result in exposures and ultimately to data compromise. Election officials commonly admit that they regard managing the election process as their primary "day job", not security.

And we are our own worst enemy. Measures taken by threat actors to compromise election systems, such as the phishing approach used in Arizona in 2016, take advantage of a general lack of situational cybersecurity awareness that results when an organization has not established a culture of information security. In the never-ending race for protecting critical data and assets, a security aware culture, both at the government level and the constituent level, is the key to long-term success.

VOTE SECURELY

In May 2018, the Senate Intelligence Committee released its interim report on election security. The committee concluded, on a bipartisan basis, that the response of the U.S. Department of Homeland Security to Russian government-sponsored efforts to undermine confidence in the U.S. voting process was "inadequate".

The committee reported that the Russian government was able to penetrate election systems in at least 18, and possibly up to 21, states, and that in a smaller subset of states, infiltrators "could have altered or deleted voter registration data," although they lacked the ability to manipulate individual votes or vote tallies. The committee wrote that the infiltrators' failure to exploit vulnerabilities in election systems could have been because they "decided against taking action" or because "they were merely gathering information and testing capabilities for a future attack".

To prevent future infiltrations, the committee made a number of recommendations, including that "at a minimum, any machine purchased going forward should have a voter-verified paper trail and no WiFi capability".

GOAL: Best-in-Class Election Process

The Office of the Arizona Secretary of State has made it clear that "Arizona takes election integrity very seriously because we need to be able to trust the outcome of our elections". While subsequent investigations have revealed that no Arizona voter data or systems were compromised in 2016, the Secretary of State, in conjunction with county election officials, realize the need for continued vigilance and improvement as cyber-attackers become more sophisticated and make use of increasingly powerful technologies in an effort to achieve the goals of their criminal or terroristic enterprises.

Following industry leading-practices, Arizona has implemented various approaches to fraud prevention including the testing of random samples of election equipment, performing monitored certification testing of all election equipment leading to the sequestering of election equipment 24-hours prior to an election, conducting full paper-based audit trails for all election transactions to facilitate hand-count verification of election tabulations, and engaging external professional services to conduct periodic physical, technical, and process vulnerability testing of the election system itself.

However, the events of 2016 exposed the need for continued investment in election process improvement and protection. The attacks on the State voter registration system identified weaknesses that required replacement of the system, a modernization initiative that nears completion. In addition, the Secretary of State appointed a full-time technology manager to oversee the end-to-end security of the election process and supporting systems. A closer working relationship was established between the Secretary's office and county election officials to facilitate the end-to-end security approach from both a centralized and distributed perspective. Finally, the Secretary is working closely with the State's Chief Information Officer and the cybersecurity office to ensure that the network infrastructure over which election processes are executed is properly monitored for threats as well as hardened and resilient against attacks.

Secretary of State Michele Reagan, Arizona's chief elections officer, said,

"the state is "light years" ahead of where it was two years ago, in terms of protecting that voter information."

Citing integration with the Trump administration's intelligence team being a step in the right direction because it signals federal agencies are on the same page.

"It shouldn't be a big shock to anyone that bad actors are still trying to get into the system," Reagan said. "I can't believe that it took everyone that long to acknowledge it."

"What do they say? 'Recognizing is the first step."

Identification of the Gaps

Just because Arizona's election systems were not successfully compromised in 2016 does not necessarily mean there was a sound and resilient protection posture against the ever-changing threat landscape. Out of the $380 million Federal HAVA Election Security Fund, more than half of which is expected to be allocated to cybersecurity, the State of Arizona received approximately $7.5 million for enhancements to the State's election system.

This additional funding enabled the Arizona Secretary of State to engage Gartner, Inc., the world's leading technology research and advisory company, to conduct an end-to-end assessment of the maturity of the State's election system security program, evaluating the completeness and effectiveness of the people, processes, and technologies currently deployed. The assessment included comprehensive threat modeling and resiliency analysis of the physical and technical protection environment using the same methodologies and tools known to be in use by today's criminal and nation-state cyber-attackers based on the latest international and domestic threat intelligence.

The results of this extensive review revealed that despite the number of security improvements made since the 2016 election, election system security remains at a reactive level. Technical controls, while extensive and effective, were not as effective as they could be due to the lack of comprehensive coverage of the controls across all aspects of the election process, as well as the use of incomplete or immature technological solutions in some cases. On a positive note, these technology-based security weaknesses represent examples of short-term technical quick wins that are currently being addressed by the Secretary.

Of greater concern are findings related to the longer-term process, organizational, and cultural challenges related to the security of elections, which is driving the reactive level of maturity. In particular, issues related to the formality of election security governance as well as a relatively weak security process structure and comprehensive ability to enforce security policy that result in significant organizational challenges.

Gartner Assessment Findings

- Strengthen and formalize processes and documentation of technology systems
- Develop standards to comprehensively manage and maintain the use of current-state technology
- Enhance software application development processes and contractor standards to ensure the level of trust required in critical software transactions
- Integrate change management processes to ensure the level of trust required in the technology infrastructure supports critical transactions with sensitive data
- Foster a culture of security awareness for internal staff as well as constituents to protect the integrity of critical transactions and sensitive data
- Define and identify critical assets to enable cost-effective protections commensurate with the risk and value of critical and sensitive software, hardware, and information
- Enhance strategies for managing user identities, mobile devices, and transaction monitoring to improve the effectiveness of existing security controls

Moving BEYOND Due Diligence

A primary tenant in cybersecurity is that compliance is not security.

A true security risk management strategy is based upon a comprehensive perspective of the security program correlated with the threat landscape, which results in a defense-in-depth AND defense-in-context protection approach.

A single security assessment based on leading risk and performance indicators, such as performed by Gartner, forms the foundation for a sound security approach that is realized by executing the resulting roadmap. However, a single assessment is simply a point-in-time perspective. To be comprehensive, true security risk management is enabled through a program of regular and periodic assessments that allow the protection approach to keep pace with the ever-changing technology and threat landscapes.

The results of the recent election system security assessment have been organized into a roadmap that enables the State of Arizona to appropriately address current and reasonably anticipated future risk over a multiyear time frame and adjust for variances in resource and funding availability.

The Arizona Secretary of State anticipates spending more than $3 million over the next few years on deployment of the recommended best-practice initiatives that address the identified weaknesses of the current-state protection environment.

1. Enable elections security through secure software development and assurance testing during the application lifecycle.

2. Establish and enforce standards for managing changes in technology to ensure that the introduction of new technology and processes do not introduce unforeseen or unaddressed risk to the election process and data.

3. Ensure that existing and new data protection best practices are used comprehensively across all aspects of the election process.

4. Assign accountable management to all aspects of the election process and enable awareness of election-specific risks to supporting systems, infrastructure, and data.

5. Leverage modern identity and access management technologies to control access to election systems based on user identity.

6. Ensure that the election network infrastructure leverages the appropriate technologies and controls to facilitates access to only authorized users, processes, systems and data.

7. Enhance and enforce physical protection for election process personnel, devices, facilities and data.

8. Monitor all election system access and transactions to ensure appropriate and authorized use of assets, as well as a timely response to security incidents.

9. Ensure that all processes, devices and systems the comprise the election ecosystem are hardened and resilient against vulnerabilities and attack.

Conclusion

While the security incident and attacks in Arizona related to the 2016 election did not result in direct impacts on vote counts or voter information, these events became a bellwether for the need to place a priority on the protection of the election process, and more importantly, strengthening citizen trust in the process and the reputation of the Office of the Arizona Secretary of State.

Admittedly, prior to 2016, security of the election process was assumed and not necessarily a focused priority. Arizona election protection has come a long way in the short time since with enhancements in the protection of election equipment, replacement of a more secure voter registration database, process audit traceability enhancements, improved election technology infrastructure, and closer coordination with security offices at the State and County.

But there is more to do.

The good news is that the "to do" list has been defined and there is now a validated plan for significant security improvements that include more focused management attention on election security; additionally enhanced and hardened hardware, software, and infrastructure; and elevated protections for access control. All to further the State's goal of Best-In-Class elections.

However, with all of these improvements, the fact that election security is not simply something that is needed during election primaries or on election day, but must become part of the day-to-day responsibilities at all levels. Vigilance in guarding against complacency once the improvements are in place, and potentially creating an environment that enables the events of 2016 to repeat. To this end, the Secretary of State is not alone in this endeavor. True, on-going election security will be dependent on improving the co-operation and collaboration with national, state, and county partners of the election process.

Security is not an end to a means. Security is process.

And while the concept of security is simple, in this day and age, achieving security is a journey for which there are no shortcuts. It is not a policy or technology that you put in place and forget. It's expensive and requires continuous investment. It takes time and requires constant attention. It forms complex relationships and is part of everything you do. And the need for it never ends.

Acknowledgements

Special thanks to the leadership at the State and Secretary of State, participating departments.

Michele Reagan, Secretary of State
Lee Miller, Deputy Secretary of State
Liz Atkinson, Chief Financial Officer
Bill Maaske, Chief Information Officer
Janine Petty, Asst. State Elections Director
Eric Spencer, State Elections Director
Matt Roberts, Director of Communications
Ken Matta, Systems Engineer

Patricia Viverto, Business Services Director
Betty McEntire, ACP Executive Director
Holly Henley State Librarian & Library Division Director
Dorie Hanson, Capital Museum Chief Administrator
Jaime Ball, Library Development Administrator
Scott Cancelosi, Director, Administrative Rules
Janet Fisher, TBL Administrator
Mala Muralidharan, E-Rate Administrator
Laura Stone, Research Library Administrator
Ted Hale, Archives & Records Division Director
Joe Morales, Help Dest Team Lead/System Administrator
Tim Jackson, Systems Engineer
Boro Yokich, Developer
Michael Schrock, Systems Engineer
Brian Schnackel, Developer
Matt Ortiz, Developer
Sara Muth, Web Developer
Tim Jackson, Systems Engineer
Jim Foster, Developer/DBA
Tony Baker, Developer

About this Report

In order to mitigate risks and vulnerabilities, the Arizona Secretary of State contracted with Gartner, Inc. to assess the level of security maturity through an extensive review of the Arizona Secretary of State's information security policies, procedures, and technologies related to elections security.

The study consisted of documentation and analysis of the current state derived from existing documentation, industry threat intelligence, and interviews with relevant subject matter experts that included management, elections, and technology perspectives. To complete the current state, Intelligence-Led Threat Testing was conducted to identify both technical and social vulnerabilities.

To address the gaps identified during the analysis phase, Gartner provided detailed recommendations and a time-phased, costed roadmap.

This report provides a high-level overview of the election-specific results, findings, and recommendations needed to advance security of the Arizona election process.