okta

Identity Management: How a Platform Approach Can Help Safeguard Elections

Identity has long been a core concern among state and local officials charged with ensuring safe, secure and accurate voting. Are voters who they say they are? Are poll workers who access voting systems adequately and appropriately credentialed?

Secretaries of state and their staffs aren't the only ones worried about identity issues as the nation rolls toward a presidential election. An NPR/PBS NewsHour/Marist poll found that about 41 percent of Americans surveyed do not think the country is prepared to protect the election system from attack. In a 2020 survey by Okta and Juniper Research, opponents of mail-in voting cited security as their number one concern.

While there are many safeguards in place to ensure voter and poll-worker identity, modernized technologies could help to further reinforce the integrity of voting systems. A platform approach to identity management could help state and local officials to better manage identity at lower cost — and with less IT intervention.

A Readiness Checklist

With the national election drawing near, state and local officials can ask themselves a number of key questions to ensure they have put in place all the needed mechanisms of identity control.

Transparency and Accountability

Identity is about security but it's also about public trust and confidence in the electoral process. Any solution to the identity management problem therefore needs to deliver a high level of transparency and accountability. When state and local agencies rely on disparate and fragmented systems to support election-related identity, it can be difficult to deliver on that high level of public visibility.

"You need an identity platform gives you a central location where there's authentication, where transactions are tracked, audited and reported," Forbes said. "Then you are able to identify when a person logged in, view their activity in the system as well as call up the security log and the audit trail."

This visibility should include not just user identities, but also the identity of devices and applications attached to the system. For complete visibility, election officials need a platform that will track when one system talks to another, how those systems access each other and the ways in which the systems pass data back and forth.

Leadership Alignment

In order to effectively manage election-related identity issues, state and local IT teams will need to win executive buy-in for the tools they are looking to use. Senior leaders across state and local government need to be aligned on the notion that identity is a key election issue, and that technology solutions including an identity management platform are a necessary component of election security.

"The most fundamental thing is just the willingness to adopt and adapt to any platform that can help state and local governments be successful in the identity space," said Mark Forreider, senior manager of solutions engineering for SLED at Okta. "It's all about recognizing you have a problem and having a willingness to move forward."

Validated Security

The systems that support voter identity must be not only intrinsically secure, but verifiably so. With a high bar of public accountability, state and local officials need to be able to explicitly demonstrate the security of their identity management solutions.

"They need solutions that have been very thoughtfully vetted out by third parties," said Thomas Bieser, vice president of Customer Solutions and Sales Engineering at Okta. "Attestation from FedRAMP, for example, is becoming increasingly important for state and sometimes local governments. The solution should have a bug bounty program, unique intellectual property, all the things necessary to support a healthy vetting process."

Scalability and Availability

Voting happens in cycles, with occasional bursts of high-volume activity. Systems that support voter and poll worker identity need to be readily scalable with ensured high availability even during the spikes.

"You have peak cycles: After 5 p.m. in each time zone, and from 8:30 to 9 in the morning," said Robert Forbes, senior solutions architect at Okta, a company that specializes in identity and access management. "So, you need on-demand scalability to handle that workload. And you need proven availability: Real availability, not availability minus planned down time and other things."

Additionally, when it comes to systems that support secure voting, the details of the service level agreement matter. Given the nature of elections — high public scrutiny, periodic bursts of intense activity — systems that support identity management need to have SLAs that go above and beyond. "In the contracts with some of the solutions providers that

> "The most fundamental thing is just the willingness to adopt and adapt to any platform that can help state and local governments be successful in the identity space. It's all about recognizing you have a problem and having a willingness to move forward."
>
> **Mark Forreider** | *Senior Manager of Solutions Engineering for SLED, Okta*

are out there, if you deploy the wrong bits to a server as part of an upgrade, that's on you. The SLA doesn't actually cover that scope," Bieser said. "There are also a lot of services out there that in their SLA do not account for downtime. You want an SLA to say: We have a zero-downtime approach."

The Path to Credible, Secure Elections

With the election just around the corner, state and local officials can take immediate action around issues of identity as a way to augment whatever protections they may already have in place.

Already in use among numerous state and local election authorities, Okta's platform solution offers an easy-to-implement approach to identity management with automated workflows that minimize the need for IT interventions.

"We are at an inflection point where we have to look at opportunities to secure elections in a meaningful way, to give real credibility to the entire process," Forreider said. "An identity platform can help state and local governments to ensure that the entire chain of data and people is secure and managed — and it helps you to avoid those bad threat actors out there trying to make an impact."

The platform includes multifactor authentication, which will eliminate some of the most common attack factors, including those that impersonate a legitimate individual logging into the system. Implementing MFA gives state and local IT teams a way to shrink that attack surface very rapidly — and it can be easily managed and deployed via Okta's identity management platform.

Additionally, a universal directory that's part of the platform helps election officials to readily manage identity for both state employees and volunteer or part-time election workers. Beyond supporting multifactor and other key authenticating mechanisms, the Okta platform also facilitates "identity proofing." In this scenario, the platform supports connections to an outside source such as a credit bureau or governmental database, against which a voter's identity is matched.

The system helps to address the thorny problem of non-payroll poll workers, the vast cadre of volunteers and others who need temporary credentials in support of the election process. A platform approach makes it easy to onboard these individuals with support for multifactor authentication, with the flexibility to tie in those identities across the various platforms state and local government may be leveraging for the election.

A FedRAMP-approved solution, the Okta platform answers the call for transparency by providing a single location and a single source of truth, along with all the needed tracking, auditing and reporting capabilities. A cloud-based solution, the platform is easily deployed, without the need for extensive effort on the part of state and local IT teams. Identity in the cloud also offers a higher level of resiliency, lessening the likelihood that a local power loss or other disruption could throw an election off course.

Okta ensures not just individual identity but also device identity, with API access management. By helping to ensure identity at all points — whether it is voter identity, poll worker identity or device identity — a platform solution can significantly reduce the risk of outside interference in elections. Moreover, state and local governments that implement a platform management solution can more readily satisfy the increasing public demand for transparency and integrity in the voting process.

Learn more about how Okta's tools can help your local government ensure election security and transparency at www.okta.com/