

Securing IT Systems for the 2024 Election Season

State & local governments are updating technologies, processes, training & procedures to ensure election security.



As state, local and territorial governments administer their elections and election infrastructure, they take different approaches using various technologies and processes. In doing so, they face common infrastructure challenges, ranging from scanner ballot readability to touchscreen system programming errors. These challenges can prolong — and at times, alter — election results.

According to the Cybersecurity and Infrastructure Security Agency, election infrastructure is critical infrastructure — encompassing cyber assets and physical assets — therefore requiring special protection. To discuss tackling these election challenges, thought leaders from government and industry spoke at a recent [FedInsider webinar](#) to share steps local and state officials can take to secure their election infrastructure.

The Complexities of the Election System

Localities around the country have election systems that are comprised of equipment, poll workers, election officials, recruiting and training processes, election preparation processes and so on. Preparing for a general election, regardless of location, requires making sure systems are up to date, functional and ready. If there have been any legal changes, localities also need to update their procedures to comply with the new laws.

“And then, they prepare for the unexpected,” said Donald Palmer, commissioner for the U.S.

Elections Assistance Commission (EAC). Considering elections are done electronically, “you must have a plan B and then a plan C ready in the event there is an issue,” he added.

A single election season can also include multiple processes, from early voting to a period where mail-in ballots are collected to election day itself. Then, a well-managed and trained staff is responsible for counting ballots and producing accurate results. “In the end, we have to get it right and then show our work,” Palmer said. “We have to ensure the security of our systems, networks and our people.”

The state of Georgia is heavily focused on security as it approaches the upcoming elections. “The physical security of our equipment and the physical security of our people, including election officials, their staff and poll workers is critical,” said Blake Evans, elections director for the Georgia Secretary of State.

After Georgia was put in the spotlight during the close 2020 election, the state turned to paper ballots to allow it to conduct proper audits. Evans said that state officials feel confident that improvements to their voting system have been fully tested and verified for the next election. Still, security is top of mind — for staff and systems — as is the spread of disinformation.

“Our processes are very transparent, which is a good thing,” Evans said, “but one of the concerns that I have occasionally is that some

Featured Experts:

■ Blake Evans

*Elections Director,
Georgia Secretary
of State*



■ Jonathan Marks

*Deputy Secretary,
Elections & Commissions,
Pennsylvania Department
of State*



■ Donald Palmer

*Commissioner,
U.S. Elections Assistance
Commission*



■ Aaron Murphy

*Field CTO for the
Americas, Veeam*



normal, small processing error that a county election official makes may be misconstrued and presented using disinformation as fraud. So, we have to make sure that we are expanding and improving processes well."

2024 Election Year Challenges

Similar to Georgia's security concerns, Jonathan Marks, deputy secretary for Elections and Commissions for the Pennsylvania Department of State, said his team is concerned about distributed denial of service attacks designed to shut down public-facing services.

He also noted a rise in engineering campaigns like phishing emails that intentionally compromise individual users to gain access to state systems. "Threats now include increasingly sophisticated foreign influence campaigns intended to undermine people's faith in elections," Marks said.

Security aside, one of the biggest concerns Marks has heading into the 2024 elections is the significant amount of turnover Pennsylvania has seen in the ranks of its county election officials. "Since 2020, over 70 county election directors or other key staff members like assistant directors or voter registration directors in more than 40 counties — so that is about two-thirds of our 67 counties — left their jobs," he said. Some were planned retirements, some were due to the pressure and the scrutiny they felt (including threats to their families) and others went to the Pennsylvania Department of State.

Marks is confident of the abilities of the new people who have since stepped into those open roles because of dedicated training programs the state designed to bring new officials up to speed to help them gain

confidence and competence. "A simple error can be used to create misinformation or disinformation," he said. "And you are going to be more at risk for that if you have a lot of turnover and election officials that do not have a lot of experience. We are committed to filling those gaps with training."

Building Election Security Resilience

When state and local governments are looking to strengthen their election security, Aaron Murphy, field chief technology officer for the Americas at Veeam, advised not getting too hung up trying to pick the best security framework to use. Instead, he said that it's best to pick one and then stick to it so that you can emphasize continuous improvement.

"The good news is that there's a lot of great material out there with agencies like the Cybersecurity and Infrastructure Security Agency, the National Institute of Standards and Technology and others all having great security frameworks," he said. "You can get on the fast-track with that knowledge, get going and get started."

CISA, for instance, has outlined how to conduct tabletop security exercises for elections, so Murphy recommended working through those questions and understanding the security posture of your chosen elections systems, and how to make them more resilient. Testing also allows teams to find gaps, vulnerabilities and put a recovery plan in place.

Evans said Georgia conducts CISA's tabletop exercises at the county and regional levels. "One of the benefits we see is that they bring local resources together and let officials talk through what can be, and in many cases will become, real-life scenarios," he said. They discuss proce-

dures, communication plans and remediation steps for situations like cyberattacks against voting systems, or what to do if threats are made against election offices and officials.

Election System Security Solutions

This year, the EAC developed a program to evaluate technologies involved in elections, like electronic polls or voter registration systems. "State and local officials want to ensure they can use a system that is approved and certified within a lab setting that's also been deployed somewhere in the county. And we want to ensure those systems are properly configured, even years after they have been deployed out into the field," Palmer said.

For Murphy, security for all systems starts with a zero-trust mindset, and then building more security onto that by adding extra verification levels. "Always know all your assets, and talk with people about how they do each of their jobs," Murphy said. Also, surround datasets with policy and compliance, enforce those policies and make sure the IT staff has access to dataset reports.

Partnering with federal agencies and acquiring the proper funding are other critical components to ensuring that state and local systems are election-ready, recently updated and able to yield timely results. Palmer recommended that localities take advantage of federal grants offered by the Help America Vote Act to refresh outdated technologies, improve cybersecurity, bolster physical security and enhance communication tools.

"We need to invest in both people and our systems," Palmer said. That will be a key to ensuring accurate and fair elections for today and into the future.



Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

☎ (202) 237-0300
✉ Info@FedInsider.com
🌐 FedInsider.com
📘 Facebook.com/FedInsiderNews
🌐 LinkedIn.com/company/FedInsider
📧 @FedInsider



Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: **Alex Kress**

☎ (703) 871-8548
✉ Alex.Kress@Carahsoft.com
🌐 Carahsoft.com/Veeam
📘 Facebook.com/Carahsoft
🌐 LinkedIn.com/company/Carahsoft
📧 @Carahsoft



Veeam
8800 Lyra Drive
Columbus, Ohio 43240
Contact: **Alex Kress**

☎ (614) 339-8200
✉ Alex.Kress@Carahsoft.com
🌐 Veeam.com/solutions/industry/government.html
📘 Facebook.com/VeeamSoftware
🌐 LinkedIn.com/company/Veeam-Software
📧 @Veeam

© 2024 Hosky Communications, Inc. All rights reserved. FedInsider and the FedInsider logo, are trademarks or registered trademarks of Hosky Communications or its subsidiaries or affiliated companies in the United States and other countries. All other marks are the property of their respective owners.

