CYBERSCOUT®

10 TIPS TO SECURE YOUR STATE'S ELECTION SYSTEMS AND VOTERS' PRIVACY

State elections boards experienced an unprecedented number of cyber attacks during the 2016 elections. The swift rise in private sector breaches signals a new era in our democracy, one where state election boards are on front lines of cyber warfare. Here's how you can begin to prepare:

1. **Find technical vulnerabilities hackers would use.** Knowing how attackers might successfully compromise your voting infrastructure is half the battle. Avoid a typical, private-sector vulnerability assessment; it might overlook key nuances in your state's election systems.

2. **Find social vulnerabilities hackers would use.** It's not enough to look for computer vulnerabilities; you must consider social engineering weaknesses, too. Your polling locations may be susceptible to a unique kind of social engineering attack due to the pressure to help constituents vote efficiently on election day.

3. **Provide clear guidance for proper security practices.** The key to security is consistent, centralized guidance and enforcement to cover all aspects of your technology, processes, and organizational controls. Every precinct must follow the same set of initiatives determined by your elections board, from the people at the polls to your state's IT department.

4. **Survey infrastructure and catalog attack surfaces.** Could an attacker compromise a third-party vendor's server before jumping to your state's voter data environment? That's already happened to one state. To prevent this from happening in your state, begin by defining the voter data environment. Inventory the architecture and devices that could pose a threat. Understanding what you have to defend will help you to keep it safe.

5. **Build a threat model to demonstrate weaknesses and shore up problems.** To help you prioritize your actions, think like your potential attackers. Who's coming after you? Russia? An opposition party? Hacktivists? Define possible threats and their likelihood. Use that prioritized list to plan out your defenses.

6. **Update post-election auditing procedures and systems.** Ensure you have positive control of the vote count from each voting machine all the way to where votes are tallied, and even after. In our experience, problems usually emerge when an organization loses track of one step in their process.

7. **Determine the most effective audit methodology and strategy.** We're entering a period of history when it will be essential for your state election board to verify voting results. That requires the implementation of risk-limiting auditing techniques unique to your state's circumstances. It should synthesize the best thinking from disciplines including statistics, privacy, security and organizational control.

8. **Define security requirements for future systems.** Whether your election board is transitioning away from paper ballots or already considering a new generation of technology, you've got to determine an authoritative set of standards by which you'll evaluate new initiatives, technologies and vendors.

7580 N Dobson Road, Suite 201
Scottsdale, AZ 85256

888.682.5911
www.CyberScout.com

Scottsdale, AZ / Providence, RI / New York, NY
Montreal, Canada / Galway, Ireland

CYBERSCOUT®

9. **Build security into design and process.** Security cannot be an afterthought; it must be baked into your process, from RFPs to implementation to maintenance. Give security the same priority as functionality and usability.

10. **Find a partner experienced in election security.** Protect voter trust in your state's election board and the freedom and fairness of your election system. Seek consulting services with experience in data breach and privacy defense as well as voting system expertise to establish the right defenses and controls ahead of time.

Feeling overwhelmed? Contact CyberScout Consulting to discuss how we can help.