Ohio election security: LaRose issues 6th statewide directive for 2025

By Mary Frances McGowan
Cleveland.com

COLUMBUS, Ohio — Ohio Secretary of State Frank LaRose issued his sixth statewide election security directive Monday, providing new cybersecurity protocols for all 88 county boards of elections.

This latest directive builds upon prior security enhancements that have positioned LaRose as the first Ohio Secretary of State to establish statewide security standards for county election boards, according to his office.

“Threats change daily, and we’re constantly adapting our protocols to stay ahead of the bad guys,” LaRose said in a statement. “We’ve positioned Ohio as the national leader on election integrity, and this new directive demonstrates our ongoing commitment to safeguarding our voting equipment and the systems that support it,”

Monday’s directive requires county boards to configure networks and equipment with the latest security updates, complete monthly cybersecurity checklists, and undergo audits by the state’s cybersecurity team — the first full-time unit of its kind in the nation, according to LaRose’s office. They must also comply with enhanced physical security requirements, including proper equipment storage, video surveillance and bipartisan access protocols.

The security audits will be led by the secretary of state’s chief information security officer and the state’s cybersecurity team. The office said its security guidance has repeatedly protected county election boards from system compromises, even as other county government systems have been breached.

The timing of this directive is significant, as it addresses an issue discovered in the lead up to the May 2025 statewide election, when an electronic pollbook was thought to be in violation of security standards. The device was never used during the election, but the Election Integrity Unit and cybersecurity team analyzed the equipment. While the investigation found no evidence of malicious intrusion, it did uncover noncompliant configurations and storage protocols that require correction before the November general election.

The announcement comes as election officials nationwide have grappled with how best to manage cybersecurity threats targeting voting infrastructure. Despite the legitimate concerns in an ever-changing technology landscape, it's worth noting that widespread voter fraud is exceedingly rare.

Noting these legitimate concerns, it is also important to note that, "the work our security teams are doing is making a real difference, and this updated guidance should reassure voters that we take seriously our duty to keep Ohio's elections accurate, accountable and secure," LaRose said.