TLP: CLEAR

Pennsylvania
Department of State

Directive Concerning Access to Electronic Voting Systems, Including But Not Limited to the Imaging of Software and Memory Files, Access to Related Internal Components, and the Consequences to County Boards for Allowing Such Access

Directive 3 of 2026
Date: April 6, 2026
Version: 1.1

Directive 3 of 2026

The following Directive is issued April 6, 2026, by the Secretary of the Commonwealth pursuant to authority contained at Section 1105-A the Pennsylvania Election Code, 25 P.S. § 3031.5. This Directive supersedes Directive 1 of 2021.

Background

The Secretary of the Commonwealth ("Secretary") has duties pursuant to Article XI-A of the Pennsylvania Election Code, Sections 1101-A through 1122-A, to examine, evaluate and certify electronic voting systems. These reviews include verifying that the voting system conforms to federal and state law and any regulations or standards regarding confidentiality, security, accuracy, safety, reliability, usability, accessibility, durability, resiliency, and auditability. The Secretary's evaluation is in addition to the federal testing and certification undertaken by the U.S. Election Assistance Commission.

The U.S. federal government has played a leading role in efforts to ensure that security and resiliency of infrastructure fulfilling unique and crucial aspects in our society are identified and protected. Executive Order 13636, issued February 12, 2013, focuses on measures required for infrastructure security. In January 2017, the U.S. Department of Homeland Security designated election infrastructure as critical infrastructure under the "Government Facilities" sector, one of the 16 critical infrastructure sectors in the United States.

The Pennsylvania Department of State recognized the significance of this designation while it was developing the security standards for certification of voting systems to be used in Pennsylvania elections. As a result, during the Department's examination, each voting system successfully completed penetration testing, access control testing, and testing to ensure that every access point and all software and firmware are protected from tampering prior to certification by the Secretary.

Access to electronic voting systems

Over the past several years, demands have been made to allow entities to have access to electronic voting systems, specifically to review and copy the internal electronic, software, mechanical, logic, and related components of such systems. These demands have included the desire to image electronic memory spaces, to download operating systems and software, and to copy information that is internal and proprietary. Such access by entities undermines chain of custody requirements and strict access limitations necessary to prevent both intentional and inadvertent tampering with electronic voting systems. It also jeopardizes the security and integrity of those systems and could negate the ability of the Secretary or electronic voting system vendors to affirmatively state that such systems continue to meet Commonwealth security standards, are validated as not posing security risks, and are able to be certified to

perform as designed by the electronic voting system vendor and as certified by both the U.S. Election Assistance Commission and the Department of State.

Limits on Access to Electronic Voting Systems

The following Directive is effective immediately:

a. **Unauthorized Access:** Unless such access complies with the requirements of "Qualified Access" prescribed herein, County Boards of Elections shall not permit or facilitate (1) physical access to voting systems or components thereof, including but not limited to internal memory, hard drives, printed circuit boards, mother boards, or other similar computer electronic boards; (2) access to any component of electronic voting systems for the purposes of copying voting systems software, source code, or proprietary data that the Department has certified with the voting system, or for the purposes of conducting penetration testing, security reviews, forensic examinations, or other vulnerability testing of an electronic voting system.

If unauthorized access occurs, the Secretary may, in his or her sole discretion, prohibit the future use of some or all of the components of that county's electronic voting system (the "compromised equipment"), without decertifying the voting system on a statewide basis. Such a prohibition applies only to the compromised equipment and does not otherwise prevent the continued use of the electronic voting system by county boards of elections. Alternatively, if the Secretary determines that the unauthorized access has compromised the security of the electronic voting system as a whole, or any related voting system, or any components thereof (collectively, individually, and in any combination, the "compromised voting system"), the Secretary may decertify (i.e., revoke the authority to use) the compromised voting system on a statewide basis. Any such decertification decision will be made in accordance with Section 1105-A(c) of the Election Code, 25 P.S. § 3031.5(c).

The Commonwealth of Pennsylvania will not reimburse any cost for replacement voting equipment for which certification or use authority has been withdrawn pursuant to this Directive. The Secretary may seek reimbursement of any costs incurred in re-examining an electronic voting system or components thereof as a result of Unauthorized Access.

b. **Qualified Access:** Nothing in this Directive is intended to limit the ability of county boards of elections to allow their elections officials to perform their duties pursuant to the Election Code or to engage vendors to assist in the maintenance and security of electronic voting systems for purposes of conducting an election as permitted by the Election Code, provided that such access is given and such functions are performed pursuant to a contract or agreement between the vendor and the county board of elections, the Department, or the manufacturer of the voting system. If the county board of elections intends to contract with a vendor that is not the manufacturer of the electronic voting system, the County Board of Elections must provide notice to the

Department 10 days in advance of the contract being executed via email to ra-stbest@pa.gov. Any such contract or agreement must provide for the vendor's indemnification of the county, the County Board of Elections, and the Commonwealth for any damage arising from such access, including the potential decommissioning or decertification of any equipment as a result thereof. Prior to such access, the vendor must agree in writing to be bound by the requirements of the Election Code, including its requirements regarding security and chain of custody of electronic voting systems. Any such access must be conducted in accordance with industry best practices, and no data, information, or reports collected during or generated from such access may be disclosed other than to the contracting county board of elections, the Department, or the manufacturer of the electronic voting system.

c. **Access sought pursuant to a valid judicial warrant:** For avoidance of doubt, this Directive's prohibition on Unauthorized Access applies with equal force to requests for Unauthorized Access to electronic voting systems or their components made by (or on behalf of) any federal, state, or local government officials without a valid judicial warrant. Like any other individual, election officials should never obstruct the execution of a valid judicial warrant, including a warrant requiring access to electronic voting systems. However, if served with a judicial warrant by a law enforcement officer, election officials must take the following steps to preserve, to the best of their ability, the security of sensitive equipment and materials and the public's interest in voter privacy and the timely certification of elections: (1) election officials should confirm that the warrant is a valid judicial warrant, *i.e.*, a warrant signed by a judge, rather than an administrative warrant; (2) election officials should request to speak to their attorneys or have the law enforcement officer speak to their attorneys, to make sure they are properly complying with the warrant and other applicable legal duties, and that the warrant is executed with the least disruption possible; (3) to the maximum extent practicable, election officials should document the execution of the warrant, including by videotaping the transfer of any data or seizure of equipment, and should ensure that an inventory is created and retained detailing precisely what equipment and data are seized, from where, and by whom; (4) election officials should make every effort to create and retain a copy of all software and data on any equipment subject to seizure. While the Secretary must ultimately evaluate the safety and usability of specific pieces of election equipment on a case-by-case basis, fidelity to chain-of-custody and security requirements make it more likely that the equipment will remain in (or can be returned to) a certified state and be approved for use in future elections.

Notice

County Boards of Elections shall notify the Secretary immediately upon receipt of any written or verbal request for access to a voting system that does not comply with the requirements of Qualified Access set forth above, including the service of warrants or any other requests from government officials. In addition, County Boards of Elections and electronic voting system manufacturers have an affirmative duty to notify the

Secretary immediately of any breach or attempted breach in the chain of custody of its voting system components, including through Unauthorized Access.

Other obligations of County Boards of Elections regarding access to election-related material

County Boards of Elections are advised to:

a. Review all contracts, lease agreements, or other documents evidencing agreements between vendors and the county to determine the contractual impacts of providing any such requested access.

b. Comply with federal law regarding the retention and preservation of records.

c. Protect the privacy of voters as required by the Pennsylvania Constitution and state law.

Future actions

This Directive shall remain in force until cancelled or rescinded by the Secretary of the Commonwealth, by a subsequent Directive, or by another issuance.

###

Version	Date	Description
1.0	07.08.21	Initial document release
1.1	04.06.26	Updated to clarify unauthorized access