



Note - Navigational menus along with other non-content related elements have been removed for your convenience. Thank you for visiting us online.

2018 Texas Election Security Update

There is no evidence that any voting or voter registration systems in Texas were compromised before the 2016 Election or in any subsequent elections.

Additionally, the [Department of Homeland Security has offered a statement](#) reiterating this fact as well.

Election security is a top priority for the Texas Secretary of State's office as we continue to employ effective and forward-thinking cybersecurity measures to further strengthen our state's elections systems and safeguard our elections infrastructure against any malicious cyber activity.

We have worked continuously to educate our election officials through both in person training and written materials on the numerous protections that are in place and are required by state law.

These safeguards include:

- No voting system is ever connected to the internet at any point - either when votes are being cast or when they are being counted. ([Section 129.054](#) Texas Election Code)
- Only software certified by the Texas Secretary of State can be loaded on a computer used for counting or accumulating vote totals. ([Section 129.055](#), Texas Election Code)
- Before and after use each day, all voting systems are sealed with locks and with seals with unique serial numbers, and all election workers must follow proper chain of custody procedures during the election, including a careful tracking of the serial numbers used to seal the machines at the end of each period of voting. (Secs. [129.051](#), [129.053](#), Texas Election Code)
- While voting is occurring, election judges are required to periodically inspect the equipment to ensure there is no tampering or damage to the equipment ([Section 125.005](#), Texas Election Code).
- All voting systems are tested three times, twice before the machines are used in the election and once immediately after. The tests consist of a deck of ballots being voted on the machines and then tabulated to ensure that the machine results are correct and match the test stack of ballots. The machines cannot be used or deployed until the test is 100% successful. Note that one of the tests conducted before the machines are used in an election is open to the public, and notice of this test is published in a local paper. Each political party has the right to submit names of individuals to represent that party on the testing board and thus every county usually has a testing board that consists of at least one person from each political party. ([Sec. 129.023](#) and [Subchapter D, Chapter 127](#), Texas Election Code).
- The election worker at the polling place (both during early voting and election day) must confirm that there are zero votes cast at the opening of voting and at the end of voting they must compare the number of ballots cast to the number of voters that have checked-in on the poll list. ([Advisory 2014-06](#), [127.068](#), Texas Election Code)
- Background checks are required for all personnel that prepare, test or service all voting system equipment. ([Sec. 129.051](#), Texas Election Code)
- Poll watchers are allowed to observe at all early voting and Election Day polling locations and at the central counting or accumulation station where ballots are being counted or vote totals accumulated. ([Chapter 33](#), Texas Election Code)
- A post-election audit (partial manual count) is required for all elections that have paper ballots ([Sec. 127.201](#), Texas Election Code).
- The Secretary of State has the authority to conduct a manual or electronic recount of any election using electronic voting systems ([Sec. 127.202](#), Texas Election Code).

These safeguards are outlined in [Section 5 of the Electronic Voting System Procedures Advisory 2014-06](#).

The Texas Secretary of State's office has also taken the following steps to further strengthen election infrastructure security in the State of Texas:

- Established effective communication protocols with the Department of Homeland Security (DHS) to coordinate cybersecurity monitoring and response.



- Engaged in a pilot program with DHS and the Multi-State Information Sharing & Analysis Center (MS-ISAC), which helped develop and improve information sharing protocols between the federal government and the states in the realm of election security.
- Instituted multi-factor authentication for election officials to ensure that only those who are authorized to do so can gain access to the statewide voter registration database.
- Installed an active Albert sensor on our voter registration database that alerts our agency when any suspicious cyber-activity occurs.
- Submitted Texas' [proposal to the U.S. Election Assistance Commission \(EAC\) \(PDF\)](#) for implementing new cybersecurity and election security measures – both at the state and local levels – using funds from the 2018 HAVA disbursement to states for election security.
- Informed and encouraged Texas counties to take advantage of free cybersecurity services and physical security assessments available from DHS, MS-ISAC, and EI-ISAC.
- Purchased licenses for a cybersecurity training course for county election officials to take prior to the November 2018 election.
- Removed legal roadblocks that prevented counties from upgrading to newer, more secure systems.

Additionally, Texas' Director of Elections, Keith Ingram, testified on Texas' election security during a Texas Senate Select Committee on Election Security hearing on February 22, 2018. [Watch the video here](#) to learn more details about our office's work to enhance the security of Texas' election infrastructure.

On November 30, 2018, the Texas Secretary of State's office submitted a Report to the Texas Legislature on Election Cybersecurity Preparedness. [Read the public summary report here \(PDF\)](#).

As always, our Elections and Information Technology officials are working tirelessly to ensure that every eligible Texas voter can cast a ballot with confidence.

Below are the full texts of selected Texas Election Code provisions that relate to election security:

Pre-Election Security Procedures: [Subchapter C, Chapter 129](#) outlines our general voting system security procedures.

Sec. 129.051. Pre-election security procedure.

- (a) The general custodian of election records shall create and maintain an inventory of all electronic information storage media.
- (b) The general custodian of election records shall develop a procedure for tracking the custody of each electronic information storage medium from its storage location, through election coding and the election process, to its final post-election disposition and return to storage. The chain of custody must require two or more individuals to perform a check and verification check whenever a transfer of custody occurs.
- (c) The general custodian of election records shall establish a secured location for storing electronic information storage media when not in use, coding a medium for an election, transferring and installing the medium into voting system equipment, and storing voting system equipment after election parameters are loaded.
- (d) An election information storage medium shall be kept in the presence of an election official or in a secured location once the medium has been coded for an election.
- (e) The general custodian of election records shall create a procedure for tracking the custody of voting system equipment once election parameters are loaded.
- (f) The general custodian of election records shall create a recovery plan to be followed if a breach in security procedures is indicated. This plan must include immediately notifying the secretary of state.
- (g) The general custodian of election records shall conduct a criminal background check for relevant election officials, staff, and temporary workers upon hiring.

Sec. 129.052. Transport of voting system equipment.

- (a) The general custodian of election records shall adopt procedures for securely storing and transporting voting system equipment. The procedures shall include provisions for locations outside the direct control of the general custodian of election records, including overnight storage at a polling location. Procedures relating to the chain of custody must require two or more individuals to perform a check and verification check whenever a transfer of custody occurs.
- (b) The general custodian of election records shall create a recovery plan to be followed if a breach in security procedures is indicated. This plan must include immediately notifying the secretary of state.
- (c) The general custodian of election records shall provide a training plan for relevant election officials, staff, and temporary workers that addresses the procedures authorized under this section.

Sec. 129.053. Access to voting system equipment.

The general custodian of election records shall secure access control keys or passwords to voting system equipment. Use of access control keys or passwords must be witnessed by one or more individuals authorized to use that information. The use of an access control key or

password must be documented and witnessed in a log dedicated for that purpose that is retained until the political subdivision disposes of the equipment.

Sec. 129.054. Network connections and wireless technology.

(a) A voting system may not be connected to any external communications network, including the Internet.

(b) A voting system may not have the capability of permitting wireless communication unless the system uses line-of-sight infrared technology that shields the transmitter and receiver from external infrared transmissions and the system can only accept transmissions generated by the system.

Sec. 129.055. Equipment and software.

The sole purpose of voting system equipment is the conduct of an election, and only software certified by the secretary of state and necessary for an election may be loaded on the equipment.

Sec. 129.056. Plan for machine failure.

The general custodian of election records shall create a contingency plan for addressing direct recording electronic voting machine failure. This plan must include the timely notification of the secretary of state.

Sec. 129.057. Use of machine in early voting.

A direct recording electronic voting machine deployed for early voting may not be deployed on Election Day.

In the polling place: Chapter 125 of the Texas Election Code provides procedures on inspecting equipment at the polling place before the polls open, during the course of the election, and after the polls close.

Sec. 125.005. Maintaining security of equipment during voting.

(a) The presiding judge shall periodically have an election officer inspect the voting system equipment for tampering and damage while voting is in process.

(b) If any tampering or damage is discovered, the inspecting officer shall immediately stop use of the equipment and report to the presiding judge, who shall promptly take appropriate action.

Sec. 125.061. Inspecting equipment at polling place.

(a) Before opening a polling place for voting on Election Day, the presiding judge shall inspect any electronic voting system equipment installed at the polling place to determine whether it is installed and functioning properly.

(b) The presiding judge shall take appropriate corrective action if the equipment is not installed or functioning properly.

Sec. 125.063. Securing equipment on close of voting.

On the close of voting at each polling place at which electronic voting system equipment is used, an election officer shall secure or inactivate the equipment as prescribed by the secretary of state so that its unauthorized operation is prevented.