Securing Elections in Citrus County

Voter Registration

- The Florida Division of Elections checks each voter registration form to verify the applicant's identity.

- The Department of State's online voter registration (OVR) website includes security measures to help ensure the identity of the voter is true and accurate while also protecting a voter's personal information. OVR requires a Florida driver's license or state ID card number and the issue date, plus the last four of the social security number.

- Our voter registration database is updated daily to remove deceased voters and felons per state notification and to identify and remove voters who have moved per county USPS notifications.

Voting

- To cast a ballot in Citrus County, a voter must be eligible and registered with a residential address in Citrus County.

- Voters must present a current and valid form of photo and signature ID to vote.

- If a voter registers by mail and has never voted in Florida, or has not been issued a Florida driver's license, Florida identification card or Social Security number, they will be required to provide additional identification prior to voting the first time.

- For mail ballots to be counted, the voter must sign the return envelope that is provided, and the voter's signature must match the one they have on file with the office.

- Florida is a paper ballot state, leaving a trail for every vote cast.

- Once a voter checks in at the polls or their mail ballot has been accepted, their record is marked as voted and will be flagged as "already voted" if they attempt to vote twice in the same election.

Tabulation and Tampering

- The Elections Office is under 24 hour camera surveillance. Doors are alarmed and monitored. We are equipped with motion sensors.

- Our state-certified voting equipment is rigorously tested before each election with a pre and public logic and accuracy test, verifying the equipment will accurately count and record votes exactly as marked. Security seals are applied to all voting equipment and documented prior to deployment to assist elections officials with detection of possible tampering.

- Individual paper results are printed at each precinct and returned to our office on Election Night to verify a match against the electronic copy.

- Precinct results are encrypted and electronically transmitted to a stand-alone server that has no connection to the internet to tabulate and report election results.

- Paper ballots are held for 22 months and can be used to verify results.

- A public manual audit is conducted after each election where ballots cast during Early Voting, Vote by Mail and on Election Day are retrieved, separated and counted. A randomly selected race and precinct is selected and a hand-count of the votes occur to make sure they match the tabulated results.

Network Security

- We purchased and installed an ALBERT Sensor, which was placed online in May of 2018. The ALBERT server monitors the network 24/7 to report any suspicious activity.

- We are running a highly rated virus software package, malware software package, and we ensure all our desktops and servers are patched and up-to-date.

- We have joined Multi-State Information Sharing and Analysis Center (MS-ISAC) and Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), and subscribed to their newsletters.

- The Department of Homeland Security (DHS) and MS-ISAC do scans to of our systems and notify us of any known vulnerabilities.

- DHS has completed a physical inspection of our current office and the future office at Meadowcrest to analyze the property and provide industry standard security protocols.

- We utilize an industry leading firewall solution that is updated, contains a list of blocked IPs and includes reporting tools to identify network security threats, issues and trends.

- Policies are in place for user passwords and use and security of office equipment.
- Cybersecurity software is in place to provide on-going cybersecurity and phishing education for both full-time and temporary employees who are on the front line of cybersecurity.