Open Letter to Voters in Volusia County

This election cycle has raised many questions about the integrity of voting equipment; whether or not my ballot will count; will my vote be changed etc. Rest assured “I have your back.” I campaigned on conducting open, honest, transparent elections and I am committed to ensuring voters, their votes count.

In Florida, we are a paper ballot state. Florida law mandates that "all voting" be by marksense ballot (with the exception for voters with special needs who may use an alternate piece of voting equipment). We can always refer to the original paper ballots, should the need arise.

Electronic voting systems are not Internet-based and do not connect to each other online; it is a closed network. Prior to each election, a Public Logic and Accuracy test is conducted of each voting tabulator and tabulation system to ensure that they are working and tabulating properly. We have tested 100% of our equipment. We conduct a public testing of the equipment in which members of the public can randomly select a voting unit to test. This was completed on October 17th in which members of the public attended; the Canvassing Board supervised the process; and an employee with the Florida Division of Elections observed.

The testing of the equipment is to ensure a vote for each candidate or issue on the ballot; counts. We test each mark for a candidate or issue and know what the results (of the testing) should be; therefore making sure the unit tabulates correctly. This includes uploading the results to ensure the whole process of tabulating and transmission of results is tested.

The individual thumb drives that record the votes from the precincts, early voting sites and vote by mail central count tabulators are digitally signed and secured. They cannot be replaced by any commercial off the shelf (COTS) thumb drive to subvert the local process of counting ballots.

Precinct tabulated results are transmitted to our office in brief encrypted burst. Outside attackers would need to overcome multiple layers of encryption which if successful, would result in corrupting, slowing or stopping the transmission of unofficial results to our office. In the unlikely event that were to happen the encrypted memory sticks could simply be imported into the results accumulation system, making the final unofficial result slower but not compromised. The final accumulations that are transmitted to the State as our unofficial results are then written to yet another memory device that are finally uploaded and transmitted to the Division of Elections on another completely separate system and network via a secure upload system which makes the likelihood that an outside attacker could subvert this process even more remote.

The final step to securing the voting process is the fact that within a week of the election, a precinct by precinct review is performed where the precinct totals tape is compared to the unofficial results transmitted on election night to verify a match and any deviations are researched and noted. Once this is completed the official result is reported.

In summary, recognizing that Florida is a paper based state which utilizes the latest state of the art electronic voting systems that are not connected to the Internet, but rather operate in a closed network leaving the likelihood of a successful breech improbable.

I place a high priority on the security of election administration, and will remain ever vigilant in identifying and reporting any future vulnerability to the elections process.