RUSSIAN ROULETTE IN VOTING

by Dr. Laura Pressley, Ph.D. who was a device engineering manager for 17 years and holds 4 U.S. patents on semiconductor device technology. She is Chair of the Travis County Republican Party Election Integrity Committee.

Ronald Regan said it best, "Trust but verify," which is more true today than ever with regard to electronic computerized voting that lacks a paper trail.

Have you ever known an elected representative who is not responsive to the majority of his constituents? Voters do not really matter if the elections are corrupt. Computerized election fraud demands to be addressed because hundreds of thousands of votes can be changed with the press of a few buttons.

Given the recent hacking of Target, T-Mobile, and Facebook, voters are becoming more aware of computer hacking. So does anyone believe that local county election offices have better security than mega-corporations? We certainly do not need the Russians or foreign ne'er-do-wells to do the hacking. All that is required are a few local county insiders with questionable ethics to enable or commit the computerized election fraud.

How does insider computerized election fraud take place since tabulation computers are typically not connected to the internet?

Remote Hacking of Modems

The largest cities use modem public phone lines or cell phone services to connect to local substations that download election results to the main central county accumulator tabulation computers. Modem passwords can be obtained through various means and allow remote access of election data for hacking.

An example of remote access software on a county's voting system was reported by the *New York Times* in Pennsylvania's Venango County. Official central counting station watchers have reported directly observing remote access of central tabulation systems in Dallas, Texas for the 2016 primary elections. Remote access has also been reported by election integrity expert, Bev Harris, for elections in Tennessee and Arizona.

Corrupt Memory Cards

Some counties use central accumulator and tabulation computers that are not connected to the internet. Vote data is downloaded by election officers to these computers via flash memory cards, called mobile ballot boxes.

An unsuspecting election officer may inadvertently download hacked election results during the normal flow of election data downloads. This specific scenario is detailed in an extensive source code review from the University of California, Berkeley under contract with the California Secretary of State in 2007.

The Berkeley report discusses one specific internal hacking method, the introduction of corrupt memory cards into the normal flow of memory cards from the precinct to the central counting computer. The report states, "this attack would potentially allow an attacker to inject false votes."

Examples of corrupt memory cards being downloaded to central counting computers have been reported in the Texas counties of Llano, Burnet, and Travis. In the 2017 general election in Travis County, audit logs from the main central accumulator computer recorded seven mobile ballot box corruption errors, "Invalid/Corrupt MBB." Election officers downloaded the corrupted card data to the main computer and did not quarantine corrupt flash cards.

When billions of dollars of county, city, state and federal programs are decided by those that are deemed the political winners, honest elections are at risk. Candidates and voters must accept that election fraud will be attempted in all its varied potential manifestations. So, how do we ensure the best election integrity?

Sequential Numbering of Ballots

The most secure voting systems utilize uniquely numbered paper ballots. This numbering system maintains the secrecy of the vote, while at the same time provides a paper backup record to validate reported results.

When county election officers are mandated to number all ballots — as required by the Texas Constitution and Election Code — counties must provide tracking and accounting of where the ballots are, trace how many are provided to polling locations, and how many are returned not used. Sequential numbering ensures there are no duplicate ballots or missing ballots. The unique sequential numbering of ballots is the most powerful method for ensuring election security and should be a federal election law mandate.

Elections Officers Must Obey the Law

When election officers strive for meticulous adherence to all election procedures and laws, such as retaining backup records, completing audits, and performing exhaustive mandatory checks and balances of all data sets, then voter and insider fraud scenarios can be prevented and discovered if they do occur.

Our duty as voters and candidates is to hold state and county election officers to the strictest adherence of all of our federal and state election laws.

Be an Official Election Watcher

The best location for official election watchers to serve is in central counting stations when electronic votes are remotely downloaded and/or entered via flash memory cards. Hacking of the main central accumulator tabulation computer is the most dangerous method of election fraud.

Honest elections will happen when we as voters and candidates step up and embrace the opportunity to take back our elections, one county at a time.