

Brian's testimony

Over 20 years experience as IT professional

Started as programmer and later supervised IT Personnel, Managed IT projects, handled IT operations and worked with IT Security personnel.

No person in business in their right mind would use such machines this vulnerable.

Small margin elections are easily stolen. Large margin elections are not - unless someone pays for the big lie and fights against any hand recount or neighborhood canvassing.

Questions

You should begin to ask your IT personnel as well as the State DOE these question before using machines for your next election and certifying them.

1. Has the source code from Dominion/vendor been verified to be malware free? Can you have someone from your IT team investigate it? How will you certify the election if you don't know if it has been compromised?
2. In what country are the developers located who produce the code for each election? China? A foreign country? Do you know? Will Dominion tell you?
3. Have you investigated the Election Management System for malware or investigated its database for triggers that would change results? Watch Fraction Magic (video in the Lt. Gov. presentation). It shows how this can be done, even in AK.
4. Do the election officials have access to the election machine digital media (memory cards) before the election to verify that there is no malware on them? If so, have you verified this?
5. Have you verified during election time that these machines were actually not connected to the internet via any other device? Some have been found to do just that.
6. Have you verified that the modem communications from the Election machines do not go anywhere but their intended location or are you relying on someone else's word? Have you verified there was not an attack on the machines during the modem communications in previous elections or other times when the machines were connected for testing?
7. Have you verified there are no embedded chips in the machines that would allow communication to other devices in the room allowing the machines to get on the internet?
8. Have you looked thoroughly on the internet to verify that the machines the Borough uses can not have the memory card or other components replaced without touching the security locks?

Conclusion

Paper Ballots with a video recorded, televised hand count is the only way to ensure ensure election integrity, provide a means to prevent recounts, and avoid every question that we will pose to the assembly.

We can't rely on voting machines that have vulnerabilities preventing safe, secure and fair elections.