Dear Clerk

As you may be aware, the Halderman report regarding the vulnerabilities of the Dominion ICX systems in Georgia has finally been released. I wanted to let you know I am extremely concerned about the findings. You can see the full 96 page report here[1].

Some concerning aspects:

- ICX suffers from critical vulnerabilities that can be exploited to subvert all of its security mechanisms, including: user authentication, data integrity protection, access control, privilege separation, audit logs, protective counters, hash validation, and external firmware validation.
- Attackers can alter the QR codes on printed ballots to modify votes.
- Anyone can install malware with only brief physical access to the machines.
- Attackers can easily forge or manipulate the smart cards that the ICX uses to authenticate technicians, poll workers, and voters.
- Attackers can execute arbitrary code with root (supervisory) privileges by altering the election definition file that county workers copy to every BMD before each election.
- The ICX contains numerous unnecessary Android applications, including a Terminal Emulator that provides a “root shell” (a supervisory command interface that overrides access controls). An attacker can alter the BMD’s audit logs simply by opening them in the on-screen Text Editor application (Section 10).
- BMDs and scanners share the same set of cryptographic keys, which are used for authentication and to protect election results on scanner memory cards. An attacker with brief access to a single ICX or a single Poll Worker Card and PIN can obtain the county-wide keys.
- The ICX BMDs are not sufficiently secured against technical compromise to withstand vote-altering attacks by bad actors.
- BMDs can be compromised to the same extent and as or more easily than the AccuVote TS and TS-X DREs they replaced. Both systems have similar weaknesses, including readily bypassed user authentication and software validation, and susceptibility to malware that spreads from a central point to machines throughout a jurisdiction. Yet with the BMD, these vulnerabilities tend to be even easier to exploit than on the DRE system, since the ICX uses more modern and modular technology that is simpler to investigate and modify.
- The ICX’s vulnerabilities also make it possible for an attacker to compromise the auditability of the ballots, by altering both the QR codes and the human readable text.
- The critical vulnerabilities in the ICX—and the wide variety of lesser but still serious security issues—indicate that it was developed without sufficient attention to security during design, software engineering, and testing. The resulting system architecture is brittle; small mistakes can lead to complete exploitation.

In addition, Halderman developed a series of proof-of-concept attacks he outlines that alter elections.

If one professor can easily identify and exploit these systems, what can a battalion of Chinese, Iranian or Russian hackers do? Does the Secretary of State, or all Lousiana government for that matter have the cyber-expertise to combat Chinese military hackers? The recent hacking of our DMV database[2] and theft of every Louisianian’s information suggest no.

This report confirms the vulnerabilities exploited[3] by cyber experts Mark Cook, Jeff O'Donnell, Joe Oltman, and Clay Pharikh the Conservative Daily podcast exist in other states and in the underlying code of not just Dominion, but all BMD computer vendors. For your convenience, here is the 90-minute version of their explaining and exploiting some of the vulnerabilities found by Dr. Halderman to change an election, leaving no trace of their efforts.

It also confirms the findings from the analysis of the voting machines in Mesa County, Colorado (see the Mesa Reports[4]) reports authored by Jeff O'Donnel and Walter C. Daugherty.

The vulnerabilities confirmed by these experts also show how easy it is to algorithmically manipulate votes on a statewide and nationwide basis. Jeff O'Donnell's demonstrates the "Mesa pattern" he identified in cast vote records from over a dozen states in his Fingerprints of Fraud CVR analysis[5].

I encourage you to review the Halderman report and the other analysis in this letter. I would also like to meet with you to discuss these issues and my concerns with continuing to use these unsecure voting computers in our Parish.

Sincerely,

Your Constituent

Full referenced links.

1. https://storage.courtlistener.com/recap/gov.uscourts.gand.240678/gov.uscourts.gand.240678.1681.0.pdf
2. https://www.youtube.com/watch?v=kxFD5GLSam0&feature=youtu.be
3. https://rumble.com/v2gagxg-show-this-video-to-your-country-officials-machine-rigging-exposed-in-90-min.html
4. https://frankspeech.com/Bombshell-Proof-Of-Election-Machine-Manipulation
5. https://fingerprintsoffraud.com/