MEMORANDUM

TO: Anoka County Board of Commissioners and Staff

FROM Anoka County Election Integrity Team (ACEIT)

DATE: September 12, 2023

SUBJECT: Why the Legitimacy of Technologically Processed Elections Must Always Be Questioned

PRESENTER: Troy Cooper

Introduction

Since the 2016 election, there has been a significant amount of talk regarding the legitimacy of our elections. What anyone happens to personally believes about their legitimacy is really irrelevant though, because there are three inescapable and indisputable facts that necessarily require us to question the legitimacy of any technologically processed election.

Analysis

The first indisputable fact is that corrupt actors, both foreign and domestic, have and will continue to seek to manipulate and subvert the legitimate outcomes of elections in our country.

- **Lessons learned from 2016, but US faces new election threats** (https://apnews.com/article/ap-top-news-elections-voting-hillary-clinton-hacking-502ea2d593ed7ae74162c8eb46290b8a)

- **Amy Klobuchar: Concerned That A 2018 Election Hack Could Succeed (Full) | Meet The Press | NBC News** (https://www.youtube.com/watch?v=9wtUxqqLh6U)

- **Democrat Senators December 2019 Letter to Dominion Voting Systems** (https://www.warren.senate.gov/imo/media/doc/H.I.G.%20McCarthy,%20&%20Staple%20Street%20letters.pdf)

The second fact, which I can personally attest to as an IT professional with decades of experience working primarily in the highly regulated and secure financial sector, is that there is absolutely NO technological system that can be adequately secured from intrusion. ABSOLUTELY NONE.

- **Could the 2016 Election Be Stolen with Help from Electronic Voting Machines?** (https://www.youtube.com/watch?v=OvF213popIA)

- **America's Voting Machines Are Extremely Vulnerable to Hacking | NowThis** (https://www.youtube.com/watch?v=BLtHW0G7DIs)

- **Why Electronic Voting Is Still A Bad Idea** (https://www.youtube.com/watch?v=LkH2r-sNjQs)

The third, and arguably the most significant fact, is the undeniable and inherent complexity associated with the current electronic voting and communication infrastructure, which is effectively an electronic "black box" that sits between our intended will as legal voters, and the purported outcome of any given election.

- **Chinese parts, hidden ownership, growing scrutiny: Inside America's biggest maker of voting machines** (https://www.nbcnews.com/news/all/chinese-parts-hidden-ownership-growing-scrutiny-inside-america-s-biggest-n1104516)

- **'Online and vulnerable': Experts find nearly three dozen U.S. voting systems connected to internet** (https://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436)

- **ES&S System Configuration** (https://leanpub.com/site_images1/sim2020/744CBCB6A352414C8B14F19CDEC6E645.png)

Conclusions/Recommendations/Summary

Election systems (and the associated outcomes of elections) are obvious high-priority targets for foreign and domestic actors who understand that manipulating the outcomes of elections is probably the single most effective way to subvert a sovereign nation state and wreak havoc from within.

This is why our election process and systems must be able to be understood from end-to-end by the average voter as well as utilize secure processes that can be readily validated by the public before, during, and after an election.

Because of the undeniable and inherent complexity associated with the current electronic voting and communication infrastructure, which is effectively an electronic "black box" that sits between our intended will as legal voters and the purported outcome of any given election, it is not currently possible that any given voter can be provided any degree of certainty with regard to how their vote is being electronically processed and routed at each and every intricate step throughout the election process and associated Open Systems Interconnect (OSI) Model.

And if you don't know or understand what the OSI Model is, given its applicability and importance to electronic voting and communications infrastructures, I would submit that the case against the use of these electronic "black box" systems can be made on that single point alone.

The main problem with any technology is that it is scalable and morally agnostic. This means that if an electronic system is compromised, the entity in control can use that electronic system to commit fraud at scale and with a low likelihood of being discovered… much less held accountable.

The same is not true of paper-based manual systems such as paper poll books and hand-counts of physical ballots. While these can also be compromised to a lesser degree, the decentralized nature of these processes, and greater chance of being caught, requires far greater effort to compromise, and are subject to diminishing returns given the lack of scalability and inability to broadly change election outcomes.

It should go without saying that something as important as the election of our representative leaders and preservation of our liberties cannot be compromised for the sake of speed or ease. We should NEVER utilize ANY "black box" infrastructure given that it is a high-value target when used for elections, it can never be guaranteed secure, and this electronic infrastructure is innately opaque and not easily and natively understood and auditable by the public.

The only truly viable option we have for transparent and secure elections are via the traditional low-tech methods utilizing paper poll books and hand-counted ballots. And even these methods and processes could use additional security fortification and process transparency.

Attachments

Note: This Memorandum and Report will be emailed to Board Members, County Administrator, PRT Division Head and Elections Manager.