Testimony regarding safe ballot collection

Alec Yasinsac

Pennsylvania Senate Committee on Government, March 18, 2024

Good morning/afternoon,

Thank you for inviting me to speak today. I am Alec Yasinsac. My father was a proud Pennsylvanian and we spent many vacations here with family in my youth, so I have a strong affinity to this state. My vita is in front of you, but as a summary, I am a Computer Scientist that has served in many election system roles: Precinct voter, military voter (for 20 years), Marine voting assistance officer (twice), poll watcher, poll worker, municipal elections official, voting system security researcher, voting system designer/developer/certifying official, et al. My comments are solely mine and have not been approved by anyone.

My message today is simple and addresses two aspects of election system security: (1) Ballot collection and (2) Ballot Pool Protection.

First, let me emphasize how critical it is to maintain the integrity of ballots as they are collected. Optimally, ballot collection would be 100% secure, with only error-free, legal ballots introduced into the ballot pool. Unfortunately, there is no ballot collection method that is 100% secure.

Worse yet, fairness dictates application of *numerous different ballot collection methods* to address various special-case voters, with each different ballot collection method having security properties. Most computer scientists that study election integrity agree that the voting system type that has the best security posture while also meeting inherent election requirements such as accuracy, privacy, timeliness, transparency/auditability, cost effectiveness, etc. is hand-marked paper ballots, marked under elections official supervision in a local voting precinct, and counted by a precinct-count scanner.

Any deviation from precinct-based, hand-marked, paper ballots (which hereafter I refer to as "Precinct Voting") inherently results in the reduced security posture of the collection method. This is because Precinct Voting is widely accepted to prevent undetectable wholesale fraud even when virtually all ballots are collected via the same Precinct Voting method. All other computer-involved ballot collection systems may be susceptible to wholesale ballot fraud attacks if employed across the electorate.

The common approach to addressing electoral special cases has been to *minimize application of non-Precinct Voting methods* exclusively to the groups that need those alternate voting methods.

For example, touch screen voting has been a true blessing to disabled voters, but the *software that operates touch screen voting machines* offers attackers a broad and deep threat surface that is not manifest in Precinct Voting and that could result in wholesale ballot fraud attacks if they are employed widely across the electorate.

Similarly, Vote By Mail (VBM) supports our military members and various other groups that naturally cannot vote in-precinct. However, VBM suffers from, among many others, the dangerous threat surface that *it is impossible to maintain a rigorous chain of custody* of either blank or voted VBM ballots.

As long as the number of voters that engage non-Precinct Voting methods remains small, the risk of malice impacting electoral outcomes through those alternate methods is also small. To say it another way for emphasis, *where application of a non-Precinct Voting method is small, potential malicious impact resulting from the inherent vulnerability in those voting methods is also small*.

Testimony regarding safe ballot collection

Alec Yasinsac

This is the foundation of my message to you today. Ballot Marking Devices (BMDs) certainly offer some positive ballot collection aspects. However, BMDs have inherent security vulnerability that cannot be ignored. While they are well-suited for use by, e.g. disabled voters, their security properties limit their safety if used across the electorate.

A quick word about computer ballot collection and wholesale fraud. The core issue is how the "ballot of record" is created. If all ballots that are collected are physically marked by voters, in a local polling place, and are inserted in the scanner by that voter, then as long as strong voter authentication practices are employed, the risk of wholesale fraud during Precinct Voting ballot collection is minimal.

On the other hand, if a computer creates or holds the official [electronic] ballot, the risk of wholesale fraud dramatically expands. That is because computer software is inherently difficult to understand and protect. Many computer scientists (including myself) have: (a) Written software that can modify voting machines causing them to alter voter selections on electronic ballots with little risk of detection and (b) Have also shown ways to integrate such malicious software into active voting machines. The best available science indicates that a single segment of malicious code could be replicated across many systems, to attack many ballots, across many jurisdictions; thus, the "wholesale" nature of computer-based fraud.

To my knowledge, no such attack has ever occurred in a real governmental election in the US, or at least none has never been detected or proven. There is no way to "test" attack science in a real election, so unfortunately, the best evidence that we have comes from the laboratory environment. However, because the impact of undetectable wholesale ballot fraud could be catastrophic, it makes sense to go to great lengths to avoid the wholesale attack vulnerability that non-Precinct Voting ballot collection methods bear by limiting their use to the greatest extent possible.

If we engage the task of ranking voting systems by security posture, I would rank BMDs right behind Precinct Voting, i.e. *BMDs are probably the second safest voting system type*. The key to that is that BMDs can be configured to allow the voter to hold the printed ballot in their hands and verify their selections before introducing it into the collected ballot pool. (BMDs not configured to provide every voter their marked ballot in their hand are well down the safety ranking ladder).

The challenge with BMDs is that there is strong research that indicates that voters are not good at verifying a voted ballot that is printed for them. So, if BMD is engaged across the majority of the electorate, it is subject to wholesale ballot fraud attacks. In my opinion, such attacks would be unlikely and difficult to enact but, also in my opinion, *it is not worth the wholesale risk of using BMDs for the broad voting population*. On the other hand, limiting BMDs to a small percentage of voters eliminates the risk of wholesale BMD ballot fraud.

Before exiting the subject of ballot collection, let me point out that VBM is by far the least secure ballot collection method that is widely used in local, state, and federal elections today. If employed broadly as Universal or No-Excuse Vote by Mail, it is subject to wholesale VBM ballot fraud attacks as is illustrated in recently reported systematic VBM fraud incidents in Connecticut, Massachusetts, and New Jersey [1, 2]. Wholesale VBM fraud is worsened by employing "authorized agents" and unsupervised drop boxes. As with BMDs, it is not worth the wholesale risk of using Vote By Mail for the broad voting population. However, limiting Vote By Mail use to a small percentage of voters, as it was originally intended, eliminates the risk of wholesale VBM fraud.

Testimony regarding safe ballot collection

Alec Yasinsac

The second aspect of election security that I address, though only briefly, is the importance of protecting the integrity of collected ballots, *post-collection*.

Neither Risk Limiting Audits nor any other audit method can detect *errors or malice that is embedded in the pool of collected ballots*. This is true whether the pollution occurs during ballot collection or after the ballot collection period has concluded.

To be clear, if a paper ballot pool becomes tainted in a way that changes an election outcome, a *Risk Limiting Audit against that tainted ballot pool will verify the wrong outcome*.

Ballot-stuffing attacks against paper ballots (i.e. injecting illegal ballots into the ballot pool) have been documented throughout history and new ballot-stuffing methods [3, 4] emerge regularly. Unsupervised ballot collection points are invitations for ballot stuffing attacks.

Ballot accounting (i.e. tracking each blank ballot with a strong chain of custody throughout the election) is pivotal to ballot pool integrity. Voting methods that prevent, or complicate, ballot accounting should be avoided or their use minimized.

Ensuring a rigorous *chain of custody* is critical when ballots are moved. It is necessary, but not sufficient, to know who had possession of ballots at any given time. There must be strong checks in place to ensure that nothing is added, changed, or deleted in transit.

Early voting dramatically expands the ballot pool threat surface. Thus, protection efforts must be dramatically increased for early voting to ensure that the ballot pool is not polluted by injected, changed, or deleted ballots during early voting.

Similarly, *audit processes* may expose the ballot pool to threats that are difficult to foresee or prevent. An important aspect of the ballot auditing threat picture is that during an audit, malicious parties know exactly how many votes are needed, and exactly where they need to come from, in order to manufacture their desired outcome. Thus, attackers can precisely engineer their ballot pool attacks during audit processes. Integrity protecting processes must be aggressively engaged during any audit activity.

Thank you again for inviting me to speak today. Please do not hesitate to call on me again if I can ever be of assistance and I'll be happy to take any questions when appropriate.