Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh PA 15213
March 15, 2024

Dear Honorable Members of the Senate State Government Committee,

I was statutory examiner of voting systems for the Secretary of the Commonwealth of Pennsylvania from 1980, when the first electronic voting statute was passed here, until 2000. During that time, I participated in every voting system examination conducted in in the Commonwealth. From 2004-2010 I was a consultant to the Secretary of the Commonwealth on electronic voting matters.

I testified before this Committee in March 2004 and have testified on electronic voting before the EAC, the U.S. Commission on Civil Rights, various U.S. House Committees and the U.S. Senate Committee on Rules and Administration. I have also served as an examiner of voting systems for Florida, Massachusetts, Nevada, West Virginia and Texas, the latter as the Texas Attorney General's designee for electronic voting.

I have been a faculty member in the School of Computer Science (formerly the Department of Computer Science) at Carnegie Mellon University since 1975, and taught a graduate course on Electronic Voting. I currently run a graduate program in Artificial Intelligence and Innovation. The opinions I express here are not necessarily those of Carnegie Mellon.

I have served as an expert in 20 court cases on electronic voting and on several occasions have testified on behalf of various governmental agencies, including the Pennsylvania Bureau of Elections.

As an expert in computer science and election technology with extensive experience in evaluating and advising on voting systems, I am writing to provide insights and recommendations regarding opportunities to enhance the integrity and security of voting machines, particularly focusing on ballot-marking devices (BMDs).

I am in favor of BMDs generally because they guide the voter through the ballot, prevent overvoting, warn of undervoting, produce ballots on which the voter's choices are indisputably clear (except possibly for write-in votes) and enable voting for the disabled. They are far superior to hand-marked ballots because voters in every election draw marks on ballots that are not susceptible to any reasonable interpretation. Further, if a voter overvotes a hand-marked ballot and then attempts to insert it in a scanner, it will be rejected. The voter is then given a choice whether to obtain a new ballot or have the overvoted one accepted as marked, in which case any overvoted race will not be counted. There is a strong tendency among voters to simply ask for the ballot to be accepted rather than to admit their mistake in front of onlookers at the

polling place and face the embarrassment of obtaining a replacement ballot. This situation never arises when BMDs are used.

However, I must express my concerns regarding certain all-in-one BMDs. Such devices allow the voter to make ballot selections using a touch screen, then print a physical ballot for the voter to inspect, and, upon voter approval, deposit the ballot in a ballot box. That is, the voter never touches the marked ballot. Some of these devices also tabulate ballots. All-in-ones present two potential problems that can compromise trust in the integrity of the voting process..

The first problem is that some machines print a barcode or QR code on the ballot that ostensibly represents the voter's selections, and then tabulate the ballot based on that code. (In some cases, the ballot are tabulated later on a different device, but also based on that code.) I am firmly against any voting system that relies on tabulating votes using any code that is not human-readable. Such systems stand the concept of voter verifiability on its head, rendering the voter's supposed approval of the ballot meaningless. It should be clear that any discrepancy between the voter's actual choices and the choices represented by the code will render the outcome questionable.

I am not against the use of codes, such as hash codes, printed on the ballot to detect potential alteration. What I am against is tabulating ballots based on such codes.

A second problem is that some ballot marking devices, notably the ExpressVoteXL, contain mechanisms that are at least potentially capable of altering a ballot after it has been reviewed and approved by the voter. Once approved by the voter, the ballot should NEVER be passed over printheads capable of placing additional marks on the ballot.

I hold a different perspective on the susceptibility of voting machines to hacking than some do. While it is conceivable that software or hardware vulnerabilities could exist, I have not seen any evidence that exploiting any such vulnerability could be exploited broadly. Retail hacking, in which small numbers of machines or ballot are compromised, is conceivable. However, no one has proposed a rational scenario in which large numbers of machines could be hacked, and surely not a scenario in which machines in multiple counties could be hacked. Nevertheless, it is not reality that matters so much as perception, and I support taking steps to eliminate as many potential vulnerabilities as possible to maintain public trust in the electoral process.

One such change that I strongly advocate for is the prohibition of any form of network access to a voting machine or ballot-marking device, whether wired or wireless. While such devices must have ports for loading ballot formats and for offloading results, no networking devices should be permitted. In particular, no wireless device should ever be present in any such machine, even if the manufacturer asserts that it is disabled or otherwise inaccessible.

In the past 20 years there has been a movement away from direct-recording electronic (DRE) machines in favor of precinct ballot counters (PBCs). The idea is that a paper ballot can always be used in a recount, and that such recounts are not believed possible with DREs. That premise is only viable if the voter's ballot has not been altered, replaced, or discarded between the time it was marked until the time it is recounted. Very little attention has been paid in statute to the

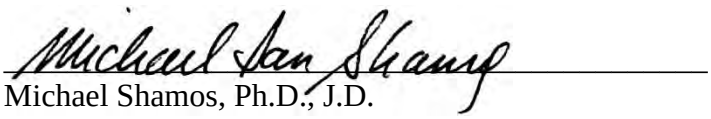
process of handling voted ballots. The Pennsylvania Election Code states only that "the judge and minority inspector shall immediately deliver the ballot boxes to the custody of the county board." No ballot-handling or secure storage procedures are provided for. This is a potential avenue for tampering that is much easier to accomplish than hacking computer systems.

It is also my opinion that the existing Voluntary Voting System Guidelines (VVSG) provided by the Election Assistance Commission (EAC) are insufficient to ensure the security and integrity of voting systems. Developments in computer and voting systems, combined with the inability of the EAC to operate effectively for political reasons, have resulted in the VVSG becoming obsolete. Comprehensive reforms are needed to establish rigorous standards and protocols that safeguard the electoral process against emerging threats and vulnerabilities. I still believe that a nationwide system of certified testing laboratories is desirable, as there is no point in having the separate states replicate each other's work, but the laboratories must be provided with up-to-date examination standards.

Lastly, I want to emphasize that raising these critical issues and advocating for change should not be construed as a critique of the hard work and dedication of election administrators and poll workers. On the contrary, most election workers share the goal of ensuring transparent and reliable elections and welcome clear procedures and reduced opportunities for ambiguity or questioning of the process. In the 120 voting system examinations I have performed, the election administrators and workers I have encountered have each been fully committed to fairness and the democratic process and would not conceive of interfering with an election. These people merit protection and severe penalties should be provided for anyone who interferes with, intimidates, or harms an election administrator or work. While I believe in the commitment and fairness of election workers, I feel that processes should be introduced to eliminate the need to rely on trust in particular election workers.

In conclusion, I urge this Committee to consider these recommendations carefully and take proactive steps to address the shortcomings and vulnerabilities in our voting systems. By prioritizing the integrity and security of our elections, we can uphold the fundamental principles of democracy and preserve the trust of the electorate.

Sincerely,



Michael Shamos, Ph.D., J.D.

Distinguished Career Professor
Director, M.S. in Artificial Intelligence and Innovation
Language Technologies Institute
School of Computer Science
Carnegie Mellon University
shamos@cs.cmu.edu