Proponent of HB 472 Ohio Votes Count Act

I am grateful for the opportunity to provide information in support of HB 472 Ohio Votes Count Act to Chairman Ghanbari, Vice Chairman Plummer, Ranking Member Thomas and members of the Homeland Security Committee, as well as sponsors Representatives Peterson and Willis, and co-sponsors Representatives Barhorst, Bird, Claggett, Click, Demetriou, Gross, King, Klopfenstein, Lear, Lipps, McClain, Wiggam, and Williams.

The bill addresses important issues regarding election systems as critical infrastructure. The point I am addressing is machine integrity. As one of the first computer science graduates in the US (from Purdue University), I have programmed in machine language (1s and 0s), as well as more advanced languages. There are many ways that code can be affected when generated and changed/hacked afterward.

How many of us have gotten a letter, perhaps from a financial institution, which said that hackers may have compromised our personal information? How many have we received over the years? I am one of the 21 million US government workers whose information was stolen about a decade ago. US government sites have been hacked more recently. CISA, the US Cyber & Infrastructure Security Agency, was hacked earlier this year and took down two of its systems (cybernews.com, March 12, 2024).

How many of us have had or know someone who had a message across the computer screen that hackers have hijacked the computer, and all will be lost if one does not call the number? Two of my friends had that happen in the past month. Unfortunately, one of them called the number, allowing the hijackers access to the computer.

How many of us have heard that large companies or organizations, such as hospitals and utility companies, experienced the same issue with ransom hijackers who demanded exorbitant amounts to give the data back or to turn the pipeline back on? Washington County PA experienced this recently and it cost them about $350,000 to get their data back. (https://www.cbsnews.com/pittsburgh/video/hackers-hit-washington-county-with-cyber-attack/ 3 min, https://www.wpxi.com/news/local/washington-county-pays-nearly-350000-ransom-hackers/4OPIETO3VBA6JBACWIG3TNVQTE/)
How many of these attacks might go unreported?

How many of us have iPhones and learned after a recent update that there was a setting turned on to share our data with any nearby iPhone? I learned of it from a high school student before I saw anything in the media. Heard nothing from Apple about it.

How many updates to apps on your phone and computer software do you get a day? A week? How many of those indicate “bug” fixes for vulnerabilities? And these are after the fact, so hackers had time to exploit these vulnerabilities before the fixes were made.

There are many examples of how election machines can be hacked or manipulated, including not updating the regular software, such as Windows; not updating the election software; and not making sure that machines adhere to the most recent government standards. I have heard that the US EAC (Election Assistance Commission, https://www.eac.gov/voting-equipment/accreditedlaboratories) only tests 1% of the source code. How safe and secure does that make us feel? And what about being connected to the internet? It is challenging to keep up with all of the possibilities that can compromise election systems.

Ohio is doing better than many states but there is room for improvement.
Please read the short article at https://news.engin.umich.edu/2018/04/mock-election/ and watch the 4:23 minute video about flipping OSU and Michigan votes at https://www.nytimes.com/video/opinion/100000005790489/i-hacked-an-election-so-can-the-russians.html.

Here is an example of hacking a voting machine in a Georgia courtroom using only a pen.
https://www.ajc.com/politics/witness-shows-how-to-tamper-with-georgia-elections-in-security-trial/WUVKCYNV3ZGOVNB6X6TDX2GEFQ/
"He also rigged the machine to print out as many ballots as he wanted."
"All in-person voters in Georgia make their choices on touchscreens that print out paper ballots."
https://www.msn.com/en-us/news/us/expert-hacks-georgia-voting-machine-in-court-revealing-potential-election-vulnerabilities/ar-BB1h9SUJ
Be very careful about the machine generating a paper ballot from the touch screen, which will always match the machine results in a recount. If hand-marked ballots are scanned, the recount compares the machine image with the hand-marked ballot. Big difference.

There are other ways to manipulate the voter rolls and ballots not included here, such as adding and deleting voter records, not reading votes correctly by tabulators and through adjudication.
https://www.pbs.org/newshour/politics/reliability-of-pricey-new-voting-machines-questioned

The Butler County Sheriff (https://www.youtube.com/watch?v=NvNukzNQawo) indicated that the Chinese, Russians, and Iranians, each try to attack and disrupt the Butler County police, fire, and sheriff systems 3-5 times a day (minutes 5:50-6:20). A Cincinnati news channel was hacked and down for weeks. They had to rely on paper. The Sheriff's system was also hacked and was down to paper. (minutes 8:58-9:10).

What if this hacking happened on Election Day? Is there a backup paper system for all Boards of Elections? Some counties, including mine, print enough paper ballots for all registered voters to vote in person but what about the precincts in other counties that only use touch screens?

Blockchain technology, suggested in HB 472, will go a long way in deterring a lot of the manipulation by tracking changes to the voter rolls and not letting voting history be deleted, as major election machine companies have done in the past when updating their election software.

If we are not yet ready to go back to all paper ballots and hand counting, which we used to do and can be done at the precinct level, then the suggestions in HB 472, and other changes can make the machines much more reliable in accurately recording and counting the votes we actually cast.

People and elected officials across the political spectrum have been concerned about the manipulation of voting data and machines over at least the last 2 decades, including elections in which members of both major parties have "won". Let's join together and fix as much as we can.

Respectfully, Martha Cooper, OSU Emeritus Professor