May 21, 2025

VIA EMAIL

Honorable Kim Reynolds
Office of the Governor
Iowa State Capitol
1007 East Grand Avenue
Des Moines, IA, 50319
Cc: Secretary of State Paul Pate, Cerro Gordo County Auditor Adam Wedmore (President, Iowa State Association of County Auditors)

Dear Governor Reynolds,

We are election integrity advocates, election auditing experts, and computer technologists whose work includes a concentration on the computer systems used to cast and count votes in the United States.

We write to urge you to veto House File 928, a bill that would make drastic and unwise changes to Iowa recount law. We urge you to reconsider this legislation and work with eleciton officials and civic groups in the coming months to draft legislation that would provide for uniform, efficient, and publicly verifiable recounts.

HF 928 prohibits candidate-funded recounts, and restricts any recount to instances of extremely small vote margins. Most troubling, HF 928 eliminates the option of a hand recount for all races except state legislative elections and local elections, and then only in extraordinary circumstances.

To begin, we note the legislative history of HF 928. Both Secretary Pate's and ISACA's lobbyists registered in favor of HF 928 on March 21, when the bill provided for a hand recount option for all elections that fell within a 1% margin of victory.[1]

On March 24, an amendment, H-1155[2], was filed, which eliminated or restricted hand recounts as described above. We do not presume to know the discussions that preceded the Secretary's and ISACA's lobbyists registering in support of HF 928, but we would appeal to Iowa's Auditors, who have long experience conducting hand recounts, to consider that the version of HF 928 introduced and reported out of the House State Government Committee preserved Iowa's tradition of allowing candidates a hand recount option. Moreover, the Secretary of State's initial proposal for making recounts uniform and efficient included a hand count option for any recount.[3]

---

[1] https://www.legis.iowa.gov/lobbyist/reports/declarations?ga=91&ba=HF928
[2] https://www.legis.iowa.gov/legislation/BillBook?ga=91&ba=H-1155
[3] https://www.legis.iowa.gov/legislation/BillBook?ba=SSB%201176&ga=91

Turning to analysis of the enrolled bill, we believe it is important to bring up a piece of recent Iowa election history, the June 2006 primary election in Pottawattamie County.

At that election, the county's election equipment and services vendor, ES&S, made a critical ballot programming error, failing to account for rotation of candidate order among precincts, and on election night, the tabulators reported facially implausible results. Auditor Marilyn Jo Drake conducted an administrative recount by hand, which reversed the outcome of several races on the ballot.

That fall, *Time* magazine quoted Drake as saying "We were just plain lucky" that the ballot programming error did not produce results that did not raise obvious red flags (boldface added in quote).[4]

> *It was just such a paper trail that enabled Marilyn Jo Drake, the auditor in Iowa's Pottawattamie County, to suss out an anomaly in a county-recorder race she was monitoring in June. She noticed that a 20-year incumbent was being beaten 10 to 1 by an unknown newcomer. Sensing a glitch, Drake cross-checked the electronic results against the totals on the paper vote and discovered the veteran was actually well ahead. The problem, it turned out, was the way the candidates' names had been ordered and coded into the access cards that activated the machines, which were made by Omaha's ES & S. Drake says she should have caught the problem in the pre-election test runs. "It was human error both on their end and my end," she notes.* ***Not every county will have an auditor as sharp-eyed as Drake--or an outcome as transparently false as the one she uncovered. "We were just plain lucky," she says.***

Pottawattamie County's issue in the June 2006 primary was caused by faulty ballot configuration and inadquate logic and accuracy (L and A)testing. It is important to note that L and A testing is not an adequate defense against a competent software attack. The 2018 report of the National Academies of Science, Engineering, and Medicine, "Securing the Vote," noted the limited scope of L and A testing (asterisks added in quote):

> *"Such pre-election testing is conducted primarily as an assurance against *non-adversarial* errors and breakdowns impacting accuracy."*[5]

---

[4] https://content.time.com/time/subscriber/article/0,33009,1552054-2,00.html
[5] https://doi.org/10.17226/25120, p. 53

Professor Alex Halderman, a University of Michigan computer scientist, noted the insufficiency of pre-election testing to prevent malware penetration in testimony to the US Senate Select Committee on Intelligence in 2017:

> *"One of the reasons why post-election audits are essential is that pre-election "logic and accuracy" testing can be defeated by malicious software running on voting machines. Vote-stealing code can be designed to detect when it's being tested and refuse to cheat while under test. Volkswagen's emission-control software did something similar to hide the fact that it was cheating during EPA test."*[6]

In recent years, election officials in Iowa and throughout the country have taken steps to isolate voting equipment, including precinct tabulators and election management systems, from the Internet. This practice is essential to election security. However, air-gapping voting equipment from the Internet, which itself depends on the care and consistency in implementation, is insufficient to secure critical IT systems. The cybersecurity firm Exeon summarizes:

> *"Despite the potentially higher security due to the lack of communication with external networks, data and networks behind air gaps are unfortunately still exposed to various cyber risks:*
>
> 1. ***Insider attacks:*** *Malicious insiders with access to the network can intentionally compromise security by introducing malware or stealing sensitive data.*
> 2. ***Physical attacks:*** *Attackers could physically enter the facility where the network is located without an internet connection to plant malicious devices or steal data.*
> 3. ***Attacks via the mobile network:*** *Sophisticated methods such as the exploitation of electromagnetic emissions or acoustic signals can potentially penetrate shielded environments.*
> 4. ***Attacks via the supply chain:*** *Malware can be introduced via hardware, e.g., routers or manipulated software, and exploit vulnerabilities of the respective manufacturer to gain access to the isolated environment.*
> 5. ***Human error:*** *Errors in manual data transfer, such as the use of infected media, can unintentionally introduce vulnerabilities or malware into the network."*[7]

Hand recounts are an essential option in today's security environment. Currently, Iowa's post-election audit law requires hand counting, but it does not provide for the results of an audit to change the outcome of an election.

---

[6] https://www.intelligence.senate.gov/sites/default/files/documents/os-ahalderman-062117.pdf

[7] https://exeon.com/blog/air-gapped-risks

The National Academies of Science, Engineering, and Medicine's 2018 report "Securing the Vote" strongly recommends hand recounts:

> *"Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots."*[8]

Regarding vulnerability to outside attack, an electronic voting system does not need to be directly connected to the Internet to be vulnerable. A regional vendor, such as Henry Adkins, which does maintenance and pre-election configuration of voting equipment in dozens of Iowa counties[9], is a critical point of vulnerability. In 2019, the Brennan Center published a report on election vendor oversight, and noted:

> *"As a 2018 U.S. Senate Intelligence Committee report observed, "State local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of [election] vendors. This limited visibility into vendors includes*
> - *vendor cybersecurity practices (how vendors protect their own information technology infrastructure and data);*
> - *foreign ownership of vendors (whether foreign nationals, or agents of foreign governments, own companies performing critical election functions);*
> - *personnel policies and procedures (whether back-ground checks and other procedures are in place to safeguard against inside attacks);*
> - *cybersecurity incident response (how vendors alert relevant authorities of attacks);*
> - *and supply chains (where parts, software patches, and installations come from; how are they transported; and how they are kept secure)."*[10]

Princeton University computer technologist Andrew Appel published a discussion of voting system vulnerability in 2016:

> *"To hack a voting machine remotely, you might think it has to be plugged in to the Internet. Most voting machines are never plugged directly into the Internet. But all voting machines must accept electronic input files from other computers: these "ballot definition files" tell the vote-counting program which candidates are on the ballot. These files are transferred to the voting machine, before each election, by inserting a cartridge or memory card into the voting machine. These cartridges are prepared on an Election Management System (EMS) computer. If that computer is hacked, then it can prepare fraudulent ballot-definition cartridges."*[11]

---

[8] https://nap.nationalacademies.org/catalog/25120/securing-the-vote-protecting-american-democracy, p. 6-7
[9] https://web.archive.org/web/20240922152733/https://www.adkins-printing.com/
[10] https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight, p. 5
[11] https://verifiedvoting.org/which-voting-machines-can-be-hacked-through-the-internet/

And the 2018 NASEM report eloquently addressed the issue of attacks on voting systems not connected to networks (boldface added).

> ***"Even when systems are not directly connected to networks, they are vulnerable to attack through physical or wireless access. They also are vulnerable whenever data transferred to them originates from another computer system that is itself vulnerable.*** *For example, to attack a voting machine that receives data only through hand-carried removable media bearing "ballot definition files," an attacker might create a ballot definition file that takes advantage of a flaw in the software that reads a ballot definition file or displays a ballot. Such an attacker need not be physically present with that removable media—entry through a network-connected computer that creates the removable storage media may suffice (the removable storage media is used to transmit the ballot definition file)."*[12]

Finally, HF 928 restricts recounts to the very smallest margins, 0.15% of ballots cast in Federal and statewide elections, and the lesser of fifty votes or 1% in all other elections. Current Iowa recount law allows any person to request a recount in precincts where they received votes.[13] We believe it is wise to allow for taxpayer-funded recounts only in close margins, but that candidates who received votes should have the option of paying for the cost of a recount, regardless of the margin of victory. States such as California, Kansas and Texas provide this option.[14]

A 2014 report, "Recount Principles and Best Practices," by a bipartisan task force led by former Washington Secretary of State Sam Reed, a Republican, and former Minnesota Secretary of State Mark Ritchie, a Democrat, strongly recommends giving all candidates the right to a recount if they pay for the cost of it:

> *"Candidates should have the option of requesting that a recount be conducted at their own expense if they lose outside the margin of eligibility for a taxpayer-funded recount. The cost of such a recount should be refunded to the candidate if the initial outcome of the race changes as a result of the candidate-initiated recount. Some states allow party officials to request a recount on behalf of a candidate."*[15]

Governor, we urge you to veto this unwise legislation, and work in the months between now and the next legislative session with Iowa's Auditors, lawmakers, civic organizations, and

---

[12] https://nap.nationalacademies.org/read/25120/chapter/7#90p, p. 90-1

[13] https://www.legis.iowa.gov/docs/code/2025/50.48.pdf

[14] https://verifiedvoting.org/recountlaws/

[15] https://web.archive.org/web/20140811040351/http://ceimn.org/sites/default/files/recountprinciplesbestpractices2014.pdf

voting technology experts to craft a recount reform law that provides the uniformity the state needs without sacrificing security, transparency, and fair access.

Respectfully,

Lynn Berry-Bernstein
Founder, Transparent Elections NC

Harvie Branscomb
electionquality.com

Paul Burke
VoteWell.net

Sean Flaherty
Chair, Iowans for Voting Integrity

Douglas W. Jones
Department of Computer Science, University of Iowa*
Retired

Neal McBurnett
https://bcn.boulder.co.us/~neal/

Barbara Simons, Ph.D

Philip B. Stark
University of California, Berkeley*

Luther Weeks
Computer Scientist
Executive Director, CTVotersCount

Tim White,
Election Integrity Advocate, Washington State

*Signature reflects the views of the signer and not those of their employer