Securing our elections: a local perspective

Presentation prepared by Dane County Clerk's Office

Scott McDonell, Dane County Clerk

The Threat of Russian Interference is Real.

The problem is real
… so what does that mean?

Some basics:

- Wisconsin Elections Systems have not been hacked.
- The 2016 recount verified the results were accurate in a contest of great interest to Russian actors.
- Every expert agrees that a paper ballot that can be (re)counted is the single best defense against hacking. That is what we have in Wisconsin.
- Beware of "Bait and Switch" arguments - equipment or systems not in use in Wisconsin.
- Finally, the main point of Russian attacks will be online: social media, WikiLeaks, as well as voter databases.

The way forward:

- Constant Vigilance is required.
- No magic bullet; no single foolproof step.
- *Creating multiple layers of defense and detection is critical.*
- ***We assume there is a problem and look for it at every step.***

The Voter Database

- Voters register all the time.
  - They must show **Proof of Address,** not only a identifying document but a geographic document to ensure they receive and vote the correct ballot.
- Online voter registration database, WisVote, is hosted and maintained by the Wisconsin Elections Commission.
- Online voter data is a vulnerability for every state.

Hackers can cause real damage:

- Release of data
- Delete or Alter data
- Compromise poll lists
- Create confusion
- Delays at polls
- Discourage voters
- Affect public confidence

WEC is securing our data:

- Upgraded hosting infrastructure
- Updated user and confidentiality agreement
- Training local clerks, including:
  - Cyber hygiene video series
  - Multi-factor authentication

Our Electoral Heritage … offers some of best defenses.

Wisconsin's Election Day Registration

- In July 2016, Illinois became aware of a breach to its registration system database. The cyber-attack reportedly included thousands of being records being viewed.
- In the 2016 New York presidential primary: more than 100,000 voters were wrongfully administratively purged from the city Board of Elections in Brooklyn.
    - This was the result of an administrative error, not hacking, but the outcomes are one and the same: **confusion and anger at the polls.**

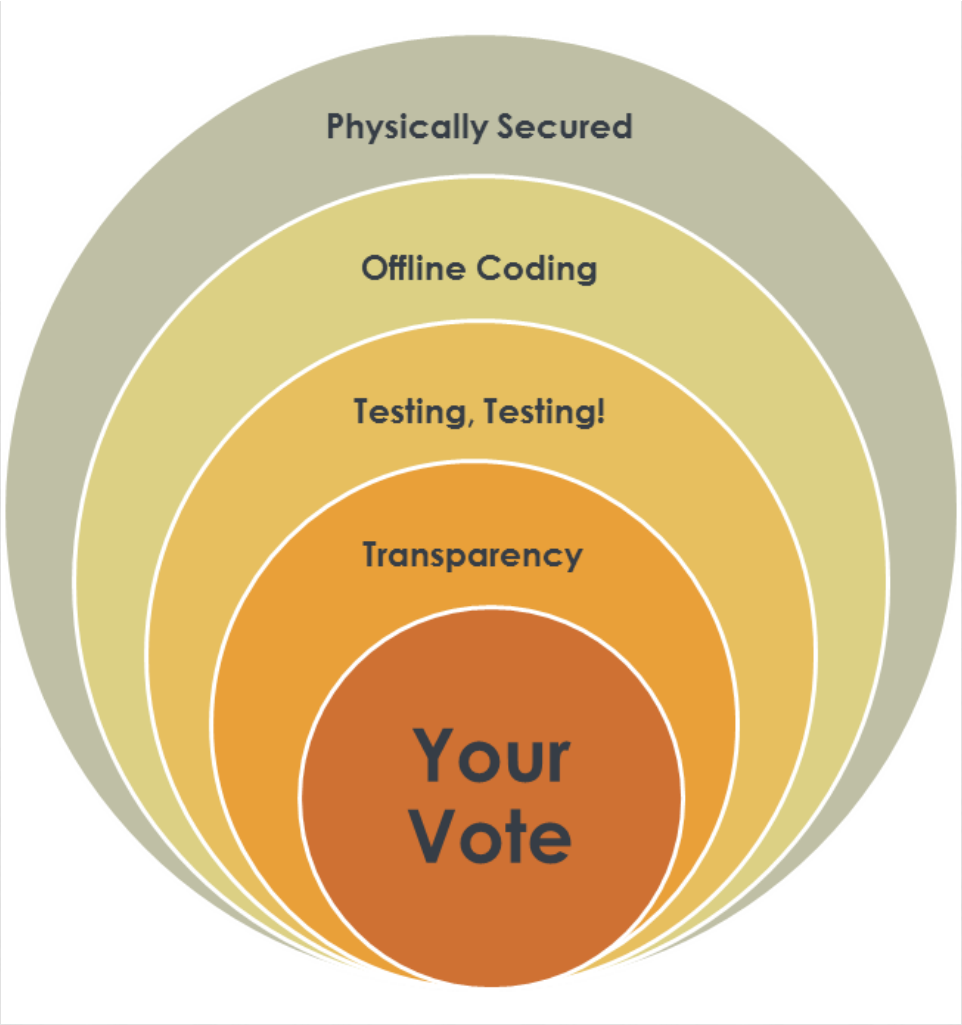
The ability to register on Election Day can neutralize this threat. It is a commonplace and trusted process.

Wisconsin's Open Primary

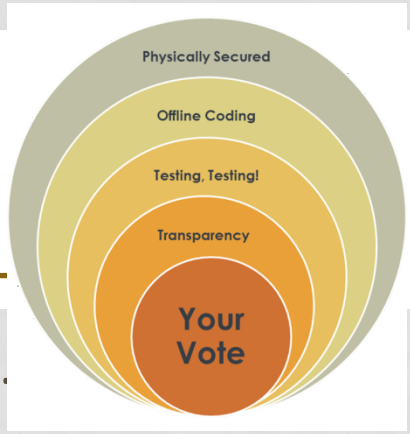
- By contrast, in many states, voters must register with a party affiliation or risk being excluded from participation. Infiltrating and altering theses records would throw a primary election into chaos.

Let's acknowledge these two policies. ***They represent a strong deterrent against hacking.***

Dane County Chronological Journey: Ballots to Audits



Step 1: Designing the Ballot



- Ballot Creation Software is offline in **locked, secured** room.
  - Stand alone computers and servers are not connected to the internet.
- Work with WEC GIS staff and County LIO Department to maintain up-to-date ward information.
  - Ballots must match WisVote district data which must match county GIS data.
- Direct relationship with all school district and municipal clerks.
  - They receive a ballot proof to **review and approve** their own races.
- Every oval position connected to a candidate is **reviewed and verified.**
- Every ballot style (combination of races contained on each ballot) is **reviewed and verified.**
- Local printer only receives a static pdf to print.
- County creates its own test deck.

Step 2: Coding the Equipment Media

- Coding is done **offline** in a **secured, locked** room. Election USB drives are stored in locked area.
- All security passwords are **chosen by county staff.**
- USB Drives are **uniquely digitally signed** for each election.
  - Every tabulator requires **authentication per every election** before it can read the election-specific USB drive.
- The county communications server, which receives the modemed totals on election night, is programmed with *exactly* the USB drives which will be used in the field on Election Day. **No more, no less.**

Step 3: County Testing and Delivery

- **Every coded USB drive is tested** by the county
  - We own 5 tabulators and run hundreds, often thousands, of test ballots.
  - Reviewing the accumulation of votes and the equipment behavior of blank ballots, over-voted races, cross-voted races (partisan primary), stray marks on ballots, write-ins, etc.
  - Testing takes days. ***We assume there is a problem to find.***

- Test results are loaded from each USB drive to the results database (mimicking election night).
- We **test the modeming process,** both the analog phone line delivery and the wireless delivery of test results.
- We **seal the USB drives** and other materials in **tamper-evident** community-specific elections bag.
- Chain of custody documentation begins.
- Elections materials, including unique **county-chosen passwords,** are **hand delivered to municipal clerks** by the county and chief deputy clerk.

Step 4: Municipal Pre-Election Role

- Municipal clerks sign county chain of custody document.
- **Secure** their elections bag from county.
- Create their own unique test decks of ballots.
- **Notice their public test,** which is held no earlier than 10 days ahead of the election. **Public is welcome** to attend.
- **Test the USB drives** (clearing the county test results, creating their own set of results).
- Modem their test results to the county (again, the intent is to mimic Election Day, **to anticipate problems ahead of time.)**
- USB drives are **sealed** in the tabulators; seal number is documented.

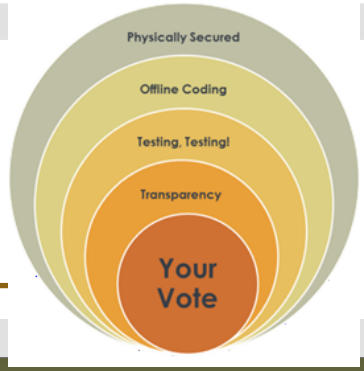
Step 5: Election Day Modeming

- Zero tapes are printed and signed by election inspectors.
- Tabulators are **NOT connected** to the internet and the out-bound modem is **NOT activated.**
  - All data generated on the devices/tabulators throughout the day is encrypted and digitally signed. Additional hash validations occur to further ensure data integrity remains intact.
- Public count of ballots is displayed on the tabulator screen. Election inspectors reconcile voters to ballots throughout the day.
- Polls close; 3 sets of results tapes automatically print.
- Election inspectors **must activate the out-bound modem.**
  - The unofficial results are transmitted using a secure communication channel between the tabulator and the communications server at the county clerk's office. The system architecture is designed so that **there is NO direct communication to the county results database.**

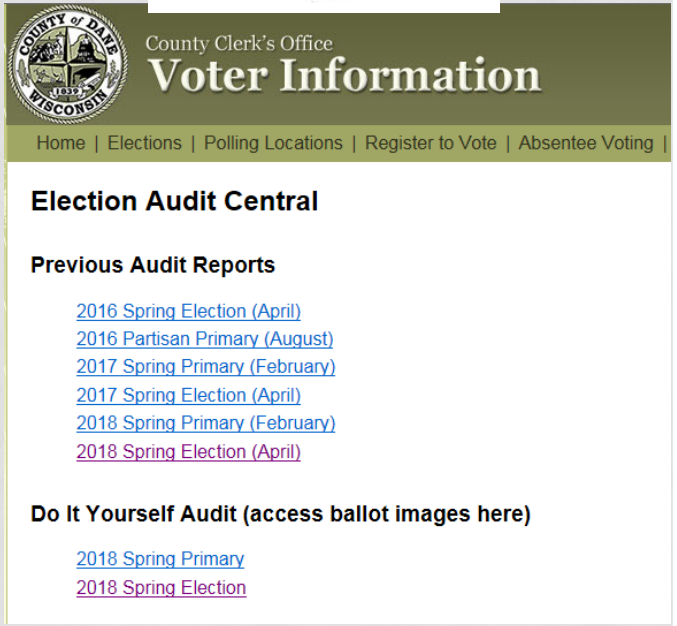
Step 6: Board of Canvass

- **The County Board of Canvass is a public meeting.**
  - One reporting unit is methodically processed at a time.
  - **It reviews every Election Day results tape,** comparing them to the modemed unofficial results received on election night.
  - Every poll book (its last voter number) is **verified** against the number of ballots.
  - Inconsistencies are researched in the Inspector Statements and municipal clerks and their inspectors are sometimes contacted to provide information/explanation.
  - The total number of voters is **compared** to the votes cast for the top-of-the-ballot race on the ballot.
  - Many processes are carried out: provisional ballot votes, review of the write-in tally sheets and votes for registered write-ins and more.
- In many ways, this process is the culmination of all our preparatory work, in ***assuming there is a problem and looking for it at every step*.**

Step 7: County Audits



- **Audit Procedures:**
  - Performed after every regularly scheduled election
  - Randomly selected two reporting units
  - Top race is hand-counted and compared to election night results tapes
  - A public meeting;
  - The final report is posted on county clerk's website.



Images:

- The actual ballot images are uploaded to website (every ballot record is completely anonymous and not connected in any way to individual voters).
- The cast ballot records are also posted.
- This level of **transparency** is unique; we welcome the public to perform their own audit.

The Positive Power of Negative Thinking

- Local clerks have multiple layers of security and detection at every step in administering elections.
- While hacking or other disruptive actions are possible, it is highly likely they would occur without detection.
- We have the ultimate safeguard: **paper ballots.**

We assume there is a problem and look for it at every step.