Frequently Asked Questions about Election Results Transmission

This document discusses some common questions and misunderstandings about the electronic transmission of election results in Wisconsin.

I. Voting Equipment Generally

A. Terms in this document.

(1) **Cryptographic Key.** In cryptography, a key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

(2) **EMS.** An Election Management System is a database management system used to enter jurisdiction information (reporting units, districts, etc.) as well as election specific information (races, candidates, etc.). In addition, the EMS is also used to lay out the ballots (list the correct contests on each ballot), program election data to be individually loaded onto tabulators, upload the results, and produce the results reports.

(3) **Firewall.** A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

(4) **IP Address.** Computer networks identify devices based on a numeric identifier called an IP (Internet Protocol) address. For example, home internet service typically has an IP address assigned by the internet service provider. Devices within the home are assigned IP addresses by the router – a machine that routes traffic within the network.

(5) **Modem.** A device that converts data from a digital format to a format for analog transmission over telephone or radio.

(6) **SFTP.** Secure File Transfer Protocol is a secure file transfer protocol that uses secure encryption to provide a high level of security for sending and receiving information.

(7) **Tabulator.** A machine used to count votes done by paper ballot. Some tabulators can communicate directly with the EMS. In Wisconsin, tabulators capable of communication can only do so before or after the election.

B. How is voting equipment certified in Wisconsin?

Equipment standards and testing information are publicly available on the Wisconsin Elections Commission website.

Before any voting system may be used in the State of Wisconsin, it must be approved in a public meeting by the six-member Wisconsin Elections Commission. The six-member WEC also reviews and certifies modem components of voting systems. Chapter EL 7 of

Wisconsin's Administrative Code governs the process. Voting Equipment may be accredited by the U.S. Election Assistance Commission (EAC) prior to its approval by the six-member Wisconsin Elections Commission, but EAC certification is not required for state certification in Wisconsin. Wisconsin Act 261 of 2015 eliminated the requirement that all voting systems approved for use in Wisconsin be accredited by the EAC.

C. What standards must voting equipment meet?

Some voting equipment contains communication hardware to transmit the results to other devices. The communications (modem) component of the voting system or equipment must be tested to the requirements contained in the most recent version or versions of the Voluntary Voting System Guidelines (VVSG) currently accepted for testing and certification by the U.S. Election Assistance Commission (EAC). Compliance with the applicable VVSG may be substantiated through federal certification by the EAC, through certification by another state that requires compliance with the applicable VVSG, or through testing conducted by a federally certified voting system test laboratory (VSTL) to the standards contained in the applicable VVSG.

Voting equipment containing telecommunications components must meet stringent standards in five evaluation areas discussed below.

(1) **Security**. All voting system functions shall prevent unauthorized access to them and preclude the execution of authorized functions in an improper sequence. System functions shall be executable only in the intended manner and order of events and under the intended conditions. Preconditions to a system function shall be logically related to the function so as to preclude its execution if the preconditions have not been met.

(2) **Accuracy.** A voting system must be capable of accurately recording and reporting all votes cast. Accuracy provisions shall be evidenced by the inclusion of control logic and data processing methods, which incorporate error detection and correction methods.

(3) **Data Integrity.** A voting system shall contain provisions for maintaining the integrity of voting and audit data during an election and for a period of at least 22 months thereafter.

(4) **Reliability.** The failure or connectivity rate will be determined by observing the number of relevant failures that occur during equipment operation. During testing, WEC staff shall maintain logs of all connection attempts. Attempts that are both successful and unsuccessful shall be noted in the logs with this information used to compile the connectivity rate. The accuracy is to be measured by verifying the completeness of the totals received.

(5) **Access to Election Data.** All systems must be capable of generating an export file to communicate results from the election jurisdiction to the Central processing location on election night after all results have been accumulated. Access to the alternate file shall in no way affect the control, processing, and integrity of the primary file or allow the primary file to be affected in any way.

D. How is voting equipment tested before Election Day?

All municipalities are required to conduct a public test of their voting equipment within 10 days *prior to* each election. Pre-election testing is intended to confirm the accuracy of voting equipment programming. This event is considered a public meeting and must be noticed at least 48 hours prior. The public is invited to attend and observe the testing process. Programming is verified by feeding a set of pre-marked ballots into each machine and reviewing the results tape that is generated. Pre-determined vote totals for each candidate in a contest for the public test should differ so that any errors in a contest can be detected. An errorless count is required at the conclusion of the process. Any anomalies identified in testing must be remedied before the equipment can be used in an election. Wis. Stats. § 5.84(1)

Wisconsin statutes also require a *post*-election audit of voting systems used in Wisconsin after each General Election. The audit is designed to assess the accuracy and performance of each voting system approved for use in the state. The audit is a public meeting and proper notice must be provided at least 48 hours in advance. A significant sample of reporting units that use each type of voting equipment are included in the selection process. The parameters of each audit are established by the Elections Commission.

During this process, elections workers conduct an independent hand count of paper ballots and tally the results of the contests. The final hand-count tally total is compared to the election night voting system results. Audit materials are submitted to WEC for review. Any discrepancies or tabulator errors are investigated by WEC staff and reviewed in a public meeting of the Commission.

II. Election Night Results Transmission

A. How are results transmitted on election night?

Only *unofficial* results are provided on Election Night. Wisconsin does not have a statewide system for reporting unofficial results on Election Night, and there is no official central website or feed where results are reported. Instead, state law requires that counties post the unofficial Election Night numbers for each polling place. The unofficial statewide and county results that the public sees on Election Night and the days thereafter come from the news media, including the Associated Press, which collects them from the 72 county clerks' websites.

To deliver the unofficial results to counties on election night, Wisconsin municipalities may choose from four options:

(1) **Hand Carry.** Municipal clerks may hand deliver the results. This option is available to all clerks and always exists as a backup to other methods.

(2) **Phone Call.** Municipal clerks may place a voice telephone call and read all of the results to the county clerk's office where the results are written on a call-in sheet. This option is also available to all clerks.

(3) **Modem Transmission.** The data may be transmitted digitally over telephone lines with a dial-up modem if the jurisdiction has the necessary equipment.

(4) **Wireless Transmission.** Data may be transmitted digitally in a wireless transmission with a cellular modem utilizing a cellular or virtual private network if the jurisdiction has purchased the necessary equipment.

B. How does the electronic transmission of data work?

In the counties where results are transmitted digitally to the county, a combination of wireless and dial-up transmission are used. Regardless of the method of transmission, or whether the modems are internal or external, all transmission components are disabled until after the close of polls. During the hours in which ballots are cast by voters, there are zero tabulators in Wisconsin with network connectivity enabled. Only after the "close polls" button on the tabulator has been pressed can election inspectors attempt to transmit unofficial results.

Transmissions from the tabulator are encrypted to prevent the data from being read or altered. In addition, tabulators include extra layers of protection not seen in other secure networked communication. For example, each signal is cryptographically signed by a key established for each election and any signals not signed will be rejected by the EMS network's security systems. The results data also has another layer of encryption that can only be decrypted by the EMS itself, after the data has reached its final destination. If an attacker tampered with these transmissions without breaking the encryption, decryption would fail and the EMS would discard the transmission. If an attacker broke the encryption, they would not be able to re-encrypt the data with the appropriate signatures and the EMS would discard the transmission.

C. Could the electronic transmission of unofficial election results be hacked?

Some theories postulate that a third-party could intercept the very brief results transmission, and break the encryption, and somehow alter the data to change election results. This narrative fails to recognize many facets of the elections process. In addition to overcoming incredible technical challenges and achieving spectacularly precise timing, the theory ignores the fact that transmitted results are encrypted with a specific security key needed to pass through the voting system firewall and also ignores the fact that the tabulator results are printed on paper. In addition, those hard copy results are further backed by paper ballots or a paper record for each and every vote. Indeed, the herculean technical feat of "hacking" the results transmission may be easily undone by a simple phone call to verify the transmission – something many Wisconsin clerks already do.

D. Is it true that an organization called WiscNet receives election results?

No. Some recent claims allege that a non-profit organization called "WiscNet" is involved in the transmission of election results. This conclusion is based on IP address attribution. Every network endpoint is assigned an IP address by which it can be identified, and the "owner" of these IP addresses is typically public record. However, the "owner" of the vast majority of IP addresses is the service provider that connects that IP address to the internet. WiscNet itself has no ability to read the encrypted results transmission. Rather, WiscNet appears providing network services for some counties receiving unofficial Election Night results.

While WEC does not have a role in managing, approving, or recommending internet service or network servicing providers used by municipalities, it appears that WiscNet has provided network services to hundreds of Wisconsin counties, municipalities, school districts, and public libraries for more than 30 years. Information about WiscNet is readily available on their website. It therefore makes perfect sense that a county IP address would appear to belong to WiscNet, in the same way a residential IP address might appear to belong to Charter Communications.

E. Could a third-party have intercepted or altered election results?

Reasonable deduction and simple logic refute nearly all possible claims of a "hack," including the following theories: whether a mysterious third-party receives unofficial election results; if a malicious algorithm was installed to switch votes; or if a hostile, foreign force obtained a connection into a tabulator before, during or after the election.

In **all** of these situations a simple recount or re-tabulation, mechanically or by hand, demonstrate the theory to be inconsistent with the facts. In 2020, recounts were undertaken in both Milwaukee and Dane Counties, and post-election audits were conducted in over 180 election reporting units, and all provided verification of the original, official results. Not one of these review efforts demonstrated a material problem with the tabulators or the software.