

**STATE OF WISCONSIN
ELECTIONS COMMISSION**

COMPLAINT FORM

Please provide the following information about yourself:

Name Peter Bernegger

Address 1806 Brynwood Trace

Telephone Number 920-551-0510

E-mail pmbmap123@gmail.com

State of Wisconsin
Before the Elections Commission

The Complaint of Peter Bernegger

_____, Complainant(s) against

Robert Kehoe a staff employee, Respondent, whose

address is 201 W Washington Ave, Madison, WI 53703

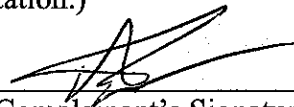
This complaint is under 5.06, & others below (Insert the applicable sections of law in chs. 5 to 10 and 12 and other laws relating to elections and election campaigns, other than laws relating to campaign financing)

I, Peter Bernegger, allege that:

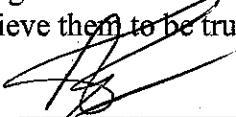
see all attached

(Set forth in detail the facts that establish probable cause to believe that a violation has occurred. Be as specific as possible as it relates to dates, times, and individuals involved. Also provide the names of individuals who may have information related to the complaint. Use as many separate pages as needed and attach copies of any supporting documentation.)

Date: November 3, 2022


Complainant's Signature

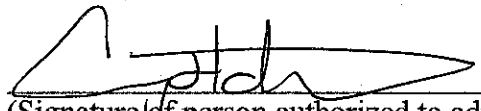
I, Peter Bernegger, being first duly sworn, on oath, state that I personally read the above complaint, and that the above allegations are true based on my personal knowledge and, as to those stated on information and belief, I believe them to be true.


Complainant's Signature

STATE OF WISCONSIN

County of Waupaca,
(county of notarization)

Sworn to before me this 4th day of
November, 2022.


(Signature of person authorized to administer oaths)

My commission expires 11/03/23, or is permanent.

Notary Public or _____
(official title if not notary)

AMY HATHORNE
Notary Public
State of Wisconsin

Please send this completed form to:
Mail: Wisconsin Elections Commission
P.O. Box 7984
Madison, WI 53707-7984
Fax: (608) 267-0500
Email: elections@wi.gov

STATE OF WISCONSIN
BEFORE THE WISCONSIN ELECTIONS COMMISSION

COMPLAINT OF:

PETER M. BERNEGGER
1806 Brynnwood Trace
New London, Wisconsin 54961

Complainant,

AGAINST

Robert Kehoe
Deputy Administrator
Wisconsin Elections Commission
201 W. Washington Avenue
2nd Floor
Madison, Wisconsin 53703

Respondent.

COMPLAINT
AND REQUEST FOR
EMERGENCY ORDER

I, as the above-named complainant, allege, upon information and belief, that probable cause exists to believe that Respondent Robert Kehoe, Deputy Administrator of the Wisconsin Elections Commission (“WEC”) has issued unlawful guidance to certain Wisconsin county and municipal clerks that creates a serious cybersecurity risk and has the potential to allow nefarious actors to manipulate the outcome of the November 8th election. Wis Stat 5.06. Mr. Kehoe is an election official. He violated the administration of elections by issuing guidance to multitudes of clerks across the state. Upon issuing the guidance, and holding a meeting with the clerks to further his guidance, he violated the conduct of elections contrary to the law. The Waukesha County Circuit Court ruled just two months ago WEC staff is barred from issuing guidance to clerks. The Wisconsin Supreme Court case of *Tiegen v WEC* ruled the same. Mr. Kehoe is a staff member, not the Commission. His email, then follow-up online meeting with the clerks the next business day, violated those court rulings. Modems have never been approved for use in Wisconsin.

FACTS

1. At 1:55 PM on Friday October 28, 2022, twelve days before the November 8th election, Mr. Kehoe sent an inaccurate and misleading email to 27 county clerks across Wisconsin giving guidance to county clerks for the purpose of hindering and restricting the public from obtaining public election materials from local election officials via legal open records requests. The WEC board did not first hold a hearing, nor did they vote to approve this guidance before it was sent by Mr. Kehoe to these clerks. See Kehoe Email; Exhibit A.
2. Municipal clerks were required to start testing election equipment on October 29th under Wis. Stat. § 5.84(1) so Mr. Kehoe's email was specifically timed to advise clerks not to cooperate in public open records requests seeking the transmission logs generated by tabulator machines during these public system tests. The log tapes are public records per Wis. Stats. 19.36(4). After the tests are complete, the machines are sealed and cannot be accessed until they are turned on again on election day so the public cannot now see transmission logs before the election begins on November 8th.
3. Mr. Kehoe's email was sent in reaction to public information derived from the open records investigation of data logs generated from a tabulator in Winnebago County. These logs clearly show the tabulators in question regularly connect to unsecured, unauthorized internet IP addresses which is in clear violation of the WEC certification of those tabulators.
4. WEC staff prepared a memorandum dated June 2, 2021 ("Staff Memo") in which it researched the system security of the proposed software upgrade to the Dominion Voting Systems (DVS) Democracy Suite 5.5-C and 5.5-CS voting systems currently used in Wisconsin. See Staff Memo in Exhibit B. The Board relied upon this report to cast a vote in approving this voting equipment.
5. In the Staff Memo, the staff makes it clear that the Democracy Suite 5.5-CS is the configuration designed to allow for the secure modeming of election results from the tabulator to the election management system (EMS) in the county clerk's office. Page 9; Staff Memo in Exhibit B.
6. The Democracy Suite 5.5-CS uses a bundled Verizon virtual private network (VPN) service consisting of a Verizon wireless cellular modem that communicates election data from the tabulator to the Verizon Secure File Transfer Protocol (SFTP) server in "the cloud" where the data is encrypted and then sent to the ImageCast Listener server which is part of the EMS located in the county clerk's office. This configuration assures the data generated by the tabulator is encrypted and transmitted securely via cell tower to the SFTP server and from there to the Listener server. This is the only data transmission path certified by the WEC for transmitting election data between the tabulator and the EMS. At no time is election data EVER supposed to be sent by the tabulator over an unsecured IP address through any network. See page 9. Staff Memo, in Exhibit B.

7. According to the 61-page Staff Memo, at no time during the transmission of tabulator data does the data come into contact with the internet. The data travels through the Verizon wireless VPN system which is designed as a cellular network system specifically to shield data from internet access where it could be intercepted or corrupted, according to the Staff Memo. The tabulator transmits data through this secure cell network directly to the county clerk via this totally secure VPN network. In Exhibit B. Verizon Wireless VPN System.
8. According to the Staff Memo, The Democracy Suite 5.5-CS system may only transfer data from the tabulator to the county clerk via the Verizon VPN network. The Staff Memo does not discuss or analyze the transfer of data through any other internet portal, or network, whatsoever. The tabulators are not authorized to connect to ANY internet IP address or server for any reason.
9. The Complainant made oral public records requests to county clerks and municipal clerks. Fond du Lac County provided an invoice for Data Services for wireless modems connected to the tabulators. See in Exhibit B. The invoice fails to state who the communications carrier is; fails to state if Verizon or Wiscnet is part of the transmissions. It has now been learned Racine County also transmits election results per a contract with Command Central, LLC. A private for-profit company unrelated to Verizon.
10. The Complainant made oral public records request to municipal clerks in Winnebago County to examine the transaction log of a tabulator in that jurisdiction. Log tapes were provided and it was discovered that the tabulator log tapes had four IP addresses on them. These included log tapes from the Nov.3rd, 2020 election. An election in 2021 and the August 9, 2022 primary. Remarkably, the county clerk receives the data through the WEC approved VPN and that IP address of Verizon is not seen on the tabulator tape. It is a breach of EMS security to have the tabulator transmit data through the internet. The tapes show the IP addresses, at least two of them, went to or through the WiscNet network. See Exhibit B; Affidavit of Parikh. He introduces as evidence the Verizon page explaining how VPN's work:
<https://www.verizon.com/articles/how-to-install-and-use-a-vpn/>
11. The Staff Memo makes it clear that the tabulators for use in Wisconsin can ONLY transmit secure, encrypted election data through the Verizon wireless VPN system or an analog modem to the Verizon SFTP and then to the Listening server at the county clerk's office where "*a firewall provides a buffer between the network segment, where the election server is located,*" and "*other internal networks which utilize separate servers.*" Page 9; Staff Memo in Exhibit B. However, this is in direct conflict with WEC not approving the use of modems.
12. As such, any and all data transmission from the tabulator directly to any IP address controlled by the county is unauthorized. The tabulator is unlawfully transmitting election data to an unknown third party or parties over unauthorized IP addresses. Two of the discovered IP addresses are those of Wiscnet. Whose office is located in Madison, WI. The tabulators are not designed to transmit election data over any IP network. Data

transmissions are restricted to the Verizon wireless modem or the analog modem connected to the Verizon VPN. Again, WEC however has never approved of the use of any modem. WEC has created its own directly conflicting decisions.

13. The transmission of data through a wireless modem is, in itself, a security risk and that is why the Federal certification authorities have not certified the use of wireless modems in electronic voting systems. Meagan Wolfe wrote, “The modeming components of Democracy Suite 5.5-CS do not meet federal certification standards.” June 2nd, 2021 report to the Board, p2. WEC is allowed by statute to approve electronic voting systems or components thereof that are not certified by federal certification authorities, but WEC did not certify modems. They thus take the risk of certifying an unsecure system.
14. The use of wireless modems, analog modems and direct IP connections introduces the likelihood of two-way communication with the tabulator and, by extension, the EMS in the county clerk’s office. Not only can election data be transmitted across unauthorized two-way networks but malware and other code can be downloaded into the tabulator and then sealed until election day. There is no way to tell at this date whether the tabulators now have malicious code installed that would allow for the transmission of election results to unauthorized third parties or even to manipulate the tabulator calculations. See Exhibit C; Declaration of Clay Parikh.
15. WEC has a duty to certify only electronic voting systems that are “*suitably designed for the purpose used, of durable construction, and is usable safely, **securely**, efficiently and accurately in the conduct of elections and counting of ballots.*” Emphasis added. Wis. Stat. §5.91 (10). It is obvious from the discovery of IP addresses on this tabulator that the electronic voting system certified by WEC does not meet the statutory requirement of “securely” as is required in statute.
16. The tabulator is not authorized to transmit election data first to an IP address and then to the Verizon VPN system, as that configuration would defeat the purpose of the VPN at the point of communication with the IP address. It was analyzed, discussed and contemplated in the Staff Memo that the Verizon VPN system was a cellular-based, end-to-end secured network for transmission of election data.
17. When the WEC commission approved the use of the Democracy Suite 5.5-CS system, it approved the list of components of that system in Appendix A of the staff memo. Conspicuously missing from the list of approved equipment is any mention of any cellular modem and specifically, the Verizon modem/VPN used across the state of Wisconsin. As such, no modems have been authorized for use by the WEC and no modeming of election data should be allowed until WEC addresses this deficiency in its certification order. See: in Exhibit B Staff Memo, Appendix A. Furthermore, there is no mention of the use of Wiscnet IP addresses in any capacity at all. Id.
18. Page 25, paragraph 11 of the staff Memo states: “*As part of this WEC certification, only equipment included in this certificate can be used together to conduct an election in Wisconsin. Previous system versions that were approved for use by the WEC, former*

Elections Board, or the former G.A.B. are not compatible with Democracy Suite 5.5-C and 5.5-CS and are not to be used in conjunction with the equipment components of Democracy Suite 5.5-C and 5.5-CS as submitted for approval. If a jurisdiction upgrades to Democracy Suite 5.5-C and 5.5-CS it needs to upgrade each and every component of the voting system to the requirements of what is approved herein.” Emphasis added. The Verizon modems used by tabulators in Wisconsin are not approved for use by the WEC because they are not listed in the approved equipment list set forth in Appendix A of the Staff Memo. Modems approved for use under earlier versions of the Democracy Suite product may not be carried forward and used. Wis. Stats. 5.91(10) does not permit the use of modems in our elections. WEC should address this defect immediately. In Exhibit B; Staff Memo; page 25

19. In his October 28, 2020 email, Mr. Kehoe admits that “... *Election observers may argue, fairly, that log tapes are public records and should be available to the public.*” but then makes a number of inaccurate claims and statements that are not only disrespectful to the public but are designed to mislead and misdirect county and municipal clerks into withholding public records. Mr. Kehoe also schedules a “meeting” with these same clerks to further discuss the inaccurate allegations he published in his illegal guidance. The WEC Board did not hold a hearing or vote to approve the guidance Kehoe gave to the clerks at this online meeting just four days ago. All of this leads to wrongful denial of access to critical election-related public records during the only time these logs can be seen by the public before the election. See Exhibit A. Kehoe violated the law by providing guidance in the email, then also during an online meeting the next business day. Id.
20. Mr. Kehoe states “*Someone recently published photographs of municipal tabulator tapes printed during a public test. When conspiracy theorists looked up the address, they discovered that it belonged to WiscNet, the county’s network service provider.*” While WiscNet may be the county’s internet service provider, WiscNet is only a network service available for general county purposes. The county clerk’s EMS is connected to a firewalled or separate internet service connected to the VPN and that IP address would not be seen through the VPN at the tabulator. Labeling any member of the public who is earnestly, ethically and legally investigating alleged election fraud is disrespectful to the public and shows bureaucratic arrogance that is unbecoming of a public SERVANT.
21. Mr. Kehoe wants the clerks to believe the county’s general internet service IP address can be seen by the tabulator when, in fact, it cannot be seen... unless it is unlawfully connected. In any event, the tabulator cannot see the clerk’s EMS connection because it is hidden through the VPN. The tabulator is not certified to transmit election data directly to any county network outside of the firewalled network connected to the listening server on the clerk’s EMS. If the tabulator is connected to the county network through the Verizon VPN, it is a massive security breach and should be investigated immediately before the November 8th election. See: Exhibit A.
22. The WEC did not certify the transmission of election data across ANY IP address or network so the tabulator should not be communication with anyone on the WiscNet

network. The tabulator was designed and approved to transmit election data across a Verizon cellular VPN which does not connect to any IP address. The only person authorized to receive election data transmitted from tabulators is the county clerk and that transmission must occur within the Verizon VPN system to assure the integrity of the election data. County clerks cannot receive election data into their EMS through any other path than the Verizon VPN and the listening server in their office.

23. Mr. Kehoe, before becoming the Deputy Administrator, was the chief technology officer of WEC. While he did not draft the Staff Memo, he has apparently not read it either because if he had, he would have immediately become suspicious when a tabulator was communicating with ANY IP address or network at all. While the tabulators using modems are not technically authorized by the WEC for use in Wisconsin because of the omission of the modem component from the Appendix A list of components, the tabulators in use in Wisconsin are not certified to connect to any data transmission path other than the Verizon VPN. They work through the Verizon VPN server which then transmits the encrypted data directly to clerks over an internet connection that cannot be seen by the tabulator. That's how VPN systems work. Any IP address discovered on a tabulator is not connected to the Verizon VPN or the clerk's well-protected EMS.
24. Mr. Kehoe realized that Winnebago County used WiscNet as its internet provider and somehow concluded that because the tabulator was communicating with an unknown third party over an unauthorized IP address on that network, the tabulator was communicating with the county. He is very wrong. The county network is separated by firewall from the EMS system in the clerks office. See Staff Memo. Page 9. No election results are ever transmitted directly from a tabulator through an unsecure and unauthorized county network to the county clerk. The system is simply not designed to work that way. Data travels from the tabulator through the Verizon VPN where it is encrypted and sent to the lister server in the county clerk's office behind a firewall. Certainly, chief technology officer and Deputy Administrator Mr. Kehoe should have instantly recognized this fact and called for an investigation of the tabulator.
25. Rather than investigate the unauthorized transfer of election data across an unsecure IP address provided, coincidentally, by the same company that provides network service to Winnebago County, Mr. Kehoe takes the opportunity to share his biased opinion with Constitutional officers in 27 jurisdictions who are trying to prepare for a very important state-wide election. Mr. Kehoe distracts their election preparation efforts by characterizing legitimate, concerned, taxpaying Wisconsin citizens as "conspiracy theorists." His allegations have resulted in county clerks contacting municipal clerks and telling them not to share legitimate public records with the public, in violation of the public's right to inspect election-related materials during the critical public testing window. In effect, he shut down public inspection of the tabulator connectivity paths just before the election. His actions prohibited the likely discovery of multiple tabulators that are somehow illegally connected to the internet via unauthorized IP addresses. Exhibit A.
26. Mr. Kehoe then makes the statement that the publication of any unauthorized IP address or network discovered on any tabulator "*heightens the risk that others may target the*

address for cyberattacks.” This statement was intended to scare the clerks into believing that somehow an unauthorized IP address discovered on a tabulator in a remote municipal location would somehow lead to a cyber-attack on the county’s general network. He does not ask why the county’s general, and publicly known network IP address is found on the tabulator or request an investigation into why tabulators designed to operate only via a Verizon VPN network has any IP address transmitting any data anywhere. Mr. Kehoe’s comment to the clerks was meant solely to distract them from preparing for the election, scare them into believing their county system will be hacked and then to deny the public the right to see if tabulators are, in fact, connected to any other unauthorized communications path. He again ignores the fact modems are not permitted by Wis. Stats. 5.91(10).

27. Mr. Kehoe then makes the extraordinarily naive statement “*while there is effectively no possibility that the results could be altered, there is some risk that transmissions could be blocked by a relatively simple and easy to execute denial of service attack.*” Mr. Kehoe, as chief technology officer of WEC should know that the tabulator data is transmitted via wireless Verizon cell modem to the Verizon SFTP server in encrypted form where it is then sent from the VERIZON SFTP server to the firewalled listening server in the clerk’s office. The tabulator cannot be attacked by a “denial of service” attack because it is not connected to the internet, at least according to WEC. And, no IP addresses should be found on the tabulator at all. There can be no “denial of service attack” against the EMS because nefarious actors would have to hack attack the Verizon VPN server and the connected listening sever which is invisible to the tabulator to get to the EMS. None of this is possible if the tabulator is not connected to the internet.
28. Mr. Kehoe than makes the incredible statement that “*this could render the EMS unable to receive transmissions on election night.*” Mr. Kehoe, had he read the Staff Memo, would realize that election data generated by tabulators using the Democracy Suite 5.5-CS software can only transmit that data through the Verizon wireless VPN network which is NOT connected to any IP address because its cellular and is transmitted directly to the SFTP server and then transmitted in encrypted form to the listening server at the clerks office. In order to block the transfer of that data to the clerk, a nefarious actor would have to hack into the Verizon VPN, discover the secure and secret IP address of the listening server, penetrate the listening server and somehow block that transmission. That... is impossible. As the tabulators are not connected to the internet, they cannot be stopped from transmitting results through the Verizon VPN to the EMS in the clerk’s office.
29. Mr. Kehoe then instructs the county clerks, constitutional officers charged with conducting a county board of canvass and certifying election results according to statute, that “*only unofficial results are provided on election night.*” Clerks are not fools. Clerks are well aware that ALL election results are “unofficial” until such time as the county board of canvass, which they chair, certifies the election results within 10 days after the election. At that point in time, election results become official. Mr. Kehoe is implying that, even if election results are hacked or manipulated or compromised, its ok, because they are only “unofficial.”

30. Mr. Kehoe then warns the clerks that “*publicly disclosing the EMS IP address increases the risk that the address will be subject to cyber-attacks.*” The IP address to the EMS is known only within the Verizon VPN and cannot be seen by anyone unless they have somehow hacked into the Verizon VPN itself. And, there should be no IP addresses in the tabulators as they are not approved by WEC to communicate with any unauthorized person across any unauthorized network. The tabulators are expected to communicate with the clerks ONLY through the very secure Verizon VPN and NEVER directly through the county internet IP.
31. If county clerks are connecting their EMS systems to IP addresses visible on the internet, they are taking massive security risk and those addresses would not be seen by the tabulator - unless the tabulator was programmed to communicate directly with the clerks via an unsecured path, rather than the Verizon VPN. One wonders why that would be the case and why the need for a Verizon VPN if the modem just skips the VPN and communicates directly with the clerk’s EMS through an unsecured IP address. It is disheartening that Mr. Kehoe fails to see the irony in his warning to the clerks. Are the modems transmitting data through the VPN as the system was designed and certified to operate and then also transmitting data to unauthorized IP addresses to unknown persons? Or, is there a second modem inside the machine that is transmitting data across the WiscNet network to unauthorized and unknown recipients? Mr. Kehoe should be investigating those possibilities rather than misleading clerks and ridiculing the public.
32. Tabulators are scattered throughout a county in multiple municipal jurisdictions. Tabulators are located in churches, public facilities, and schools. While schools and other public places may be WiscNet customers, there is no possible justification for tabulators to be connected to private networks operated by churches, schools, and other private places. So... how would a county IP address end up on a tabulator in a municipality far from the county facilities and network? There should be no connectivity between tabulators and church networks, non-profit networks or school networks at all. Are there municipal clerks transmitting on these networks? If yes, how many? What networks? Why would a tabulator designed and approved by WEC to transmit data to the Verizon VPN have to be connected to the internet at all? Verizon does not, and cannot, use a public IP address to receive data into its VPN. If it does, the system is simply unsecure and subject to hacking.
33. Mr. Kehoe then finishes with a recommendation to “*consult with legal counsel regarding the sensitivity of this data and whether you wish to release it.*” This, of course, scares the clerks in to thinking they may have a legal problem and leads to clerks advising municipal clerks not to share tabulator transmission logs with the public so as not to disclose unauthorized and illegal IP addresses discovered on tabulators. Investigators have experienced this result in multiple municipal locations since Mr. Kehoe published his email.
34. Modems have not been certified or approved for use in our elections by anyone – at all. If these uncertified modems are plugged into (or turned on if internal) a tabulator it immediately makes the entire tabulator uncertified.

PRAYER FOR RELIEF

35. WHEREFORE, Complainant respectfully requests the Wisconsin Elections Commission order the following relief:
- a. The WEC should issue an immediate emergency order prohibiting the use of any cellular modem transmission of election results in Wisconsin until such time as it can re-certify the safety and security of modeming devices used in Wisconsin;
 - b. Issue an immediate emergency order directing all county and municipal clerks to generate and publish transmission logs from all tabulators transmitting election data both before ballots are accepted into the machines on election day and then again after the polls are closed to assure the public that tabulators are not transmitting election data over any unauthorized data path to any unauthorized third party over any unauthorized data network.
 - c. The WEC should order Mr. Kehoe's email to county clerks be revoked as guidance illegally issued by staff but not approved by the WEC Commission;
 - d. Take such disciplinary action against Mr. Kehoe as warranted in light of his issuing unauthorized guidance to 27 county clerks who have been distracted and misinformed by his communication and who now have interfered with the public's right to access public records;
 - e. Take such disciplinary action against Mr. Kehoe as warranted in light of his apparent gross misunderstanding of the technology currently approved by WEC and used in 27 counties in Wisconsin;
 - f. Investigate why the Commission approved the Democracy Suite 5.5-CS system components but failed to approve the use of the necessary Verizon cellular modem component which was excluded from the component list approved devices set forth in Appendix A of the Staff Memo.
 - g. Announce to the public how many municipalities in our state are transmitting the unofficial election results on election nights using the Wiscnet network. Announce to the public when did WEC first know Wiscnet was part of our elections. Announce to the public if Verizon contracts with Wiscnet. If yes, state in detail why this is the case.
 - h. For Kehoe to fully explain why WEC staff agreed in the first place to recommend entrusting our election results to the same for-profit companies – Dominion which is owned by State Street Capital Hedge Fund and Command Central a private nonprofit – who count the votes.

From: Kehoe, Robert Y - ELECTIONS <robert.kehoe@wisconsin.gov>
Sent: Friday, October 28, 2022 1:55 PM
To: patrick.moynihan@browncountywi.gov <patrick.moynihan@browncountywi.gov>; Beth Hauser <Beth.Hauser@calumetcounty.org>; sue.moll@columbiacountywi.gov <sue.moll@columbiacountywi.gov>; kgibson@co.dodge.wi.us <kgibson@co.dodge.wi.us>; McDonell, Scott <McDonell@countyofdane.com>; jlau@co.door.wi.us <jlau@co.door.wi.us>; Sandvick, Sue <Sue.Sandvick@douglascountywi.org>; sue.mcdonald@eauclairecounty.gov <sue.mcdonald@eauclairecounty.gov>; lisa.freiberg@fdlco.wi.gov <lisa.freiberg@fdlco.wi.gov>; Arianna Voegeli <avoegeli@greencountywi.org>; audreyM@jeffersoncountywi.gov <audreyM@jeffersoncountywi.gov>; regi.waligora@kenoshacounty.org <regi.waligora@kenoshacounty.org>; Dankmeyer, Ginny <gdankmeyer@lacrossecounty.org>; jessicabackus@co.manitowoc.wi.us <jessicabackus@co.manitowoc.wi.us>; Kim Trueblood <Kim.Trueblood@co.marathon.wi.us>; Hawley, Michelle <Michelle.Hawley@milwaukeecountywi.gov>; Jeffrey.King@outagamie.org <Jeffrey.King@outagamie.org>; JWINKELHORST@CO.OZAUKEE.WI.US <JWINKELHORST@CO.OZAUKEE.WI.US>; Wendy.Christensen@racinecounty.com <Wendy.Christensen@racinecounty.com>; Lisa Tollefson <Lisa.Tollefson@co.rock.wi.us>; Becky Evert <becky.evert@saukcountywi.gov>; christine.hines@sccwi.gov <christine.hines@sccwi.gov>; spike@co.walworth.wi.us <spike@co.walworth.wi.us>; ashley.reichert@co.washington.wi.us <ashley.reichert@co.washington.wi.us>; Wartman, Meg <mwartman@waukeshecw.gov>; Ertmer, Sue <sertmer@co.winnebago.wi.us>; tminer@co.wood.wi.us <tminer@co.wood.wi.us>
Cc: Wolfe, Meagan - ELECTIONS <Meagan.Wolfe@wisconsin.gov>; Vetterkind, Riley - ELECTIONS <riley.vetterkind@wisconsin.gov>
Subject: Election Security Notice for Counties

CAUTION: This email originated from outside of Milwaukee County. Use the Phish Alert Report button to have IMSD review this message if you think it is suspicious.

Good afternoon County Clerks,

We wanted to alert you to an emerging concern so that you are familiar with the issue. We are scheduling a meeting on Monday to discuss this matter further and will send you an invitation soon.

BACKGROUND:

Someone recently published photographs of municipal tabulator log tapes printed during a public test. These tapes disclosed the IP address of the county EMS (picture below my signature block). When conspiracy theorists looked up the address, they discovered that it belonged to WiscNet, the county's network service provider. This then resulted in a narrative that WiscNet is a mysterious organization

“receiving” election results and involved in election fraud. Employees of WiscNet then started receiving angry and harassing messages from across the country. Of course, WiscNet has no ability to read encrypted transmissions going to their customers.

More critically to counties, the publication of this IP address also heightens the risk that others may target the address for cyberattacks. Compounding the risk, many people believe the IP address is associated with election fraud, so it is a “fair” target. While there is effectively no possibility that results could be altered, there is some risk that transmissions could be blocked by a relatively simple and easy-to-execute denial of service attack. This could render the EMS unable to receive transmissions on election night.

MITIGATION:

Wisconsin is already well positioned to mitigate to this risk, because county networks are generally robust and there are several options available for results reporting. Furthermore, as you all know, only unofficial results are provided on election night. That said, we recommend all counties and municipalities review their back up plans for transmitting results. In the event of a cyber-attack, equipment outage, or any other disruption, municipalities may not be able to modem. This does not impact the unofficial or official results, but unexpected delays may be frustrating for staff and voters. Please ensure your election inspectors are all familiar with your back-up plans. We also suggest that you test your back up plan for unofficial results transmittal before election day.

To address public questions about results transmission, the WEC prepared an FAQ located here: <https://elections.wi.gov/elections/voting-equipment-wisconsin/election-results-transmission>

Finally, Election observers may argue, fairly, that log tapes are public records and should be available to the public. We caution that publicly disclosing the EMS IP address increases the risk that the address will be subject to cyber-attacks. As a result, you may wish to consult with legal counsel regarding the sensitivity of this data and whether you wish to release it.

Please let me know if you have any questions, otherwise we hope to discuss this further next Monday in a short call. Thank you and have a good weekend!

Robert Kehoe
Deputy Administrator
Wisconsin Elections Commission
Phone - 608.261.2019
Fax – 608.267.0500
robert.kehoe@wisconsin.gov
<https://elections.wi.gov>

[cont. -]

```
INFO - [File Transfer] Socket
timeout while connected on message

09 Aug 2022 20:48:22:249
[FTServerThread] ssltransfer.cpp(475)
ERROR - [File Transfer] The socket
operation timed out
09 Aug 2022 20:48:22:119
[FTServerThread] ssltransfer.cpp(529)
INFO - [File Transfer] Connection
enters in encrypted mode
09 Aug 2022 20:48:20:326 [Main
thread] ftmanagerimp.cpp(362) INFO -
[File Transfer] Transfer started. The
total number of files is 1

09 Aug 2022 20:48:20:291
[FTServerThread] ssltransfer.cpp(501)
INFO - [File Transfer] Connection to
the host 216.56.██████ has been
achieved.

09 Aug 2022 20:48:20:290
[FTServerThread] ssltransfer.cpp(614)
INFO - [File Transfer] A connection
is established.
09 Aug 2022 20:48:20:254
[FTServerThread] ssltransfer.cpp(204)
```

Declaration of Clay U. Parikh

I, CLAY U. PARIKH, declare under penalty of perjury that the following is true and correct:

1. I have personal knowledge of the matters set forth below and would testify competently to them if called upon to do so.

2. I have a Master of Science in Cyber Security, Computer Science from the University of Alabama in Huntsville. I have a Bachelor of Science in Computer Science, Systems Major from the University of North Carolina at Wilmington. In February 2007 I obtained the Certified Information Systems Security Professional (CISSP) certification and have continually maintained good standing. I also hold the following certifications; Certified Ethical Hacker (CEH) and Certified Hacking Forensic Investigator (CHFI).

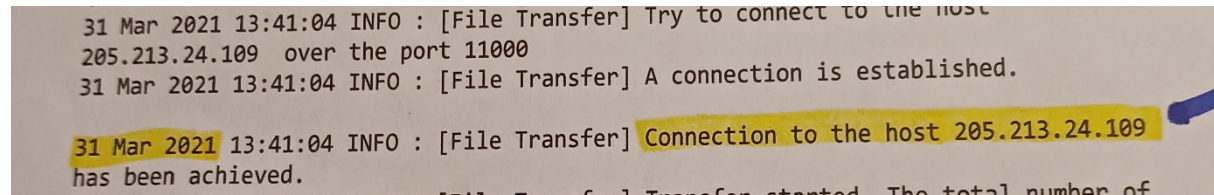
3. Since December of 2003, I have continually worked in the areas of Information Assurance (IA), Information Security and Cyber Security. I have performed and led teams in Vulnerability Management, Security Test and Evaluation (ST&E) and system accreditation. I have supported both civil and Department of Defense agencies within the U.S. government as well as international customers, such as NATO. I have served as the Information Security Manager for enterprise operations at Marshall Space Flight Center, where I ensured all NASA programs and projects aboard the center met NASA enterprise security standards. I was also responsible in part for ensuring the Marshall Space Flight Center maintained its Authority To Operate (ATO) within the NASA agency. I have also served as the Deputy Cyber Manager for the Army Corps of Engineers where I led and managed several teams directly in: Vulnerability Management, Assessment and Authorization (A&A), Vulnerability Scanning, Host Based Security System (HBSS), Ports Protocols and Service Management, and an Information System

Security Manager (ISSM) team for cloud projects. I also have performed internal digital forensic audits. During this time span, I also worked at the Army Threat Systems Management Office (TSMO) as a member of the Threat Computer Network Operations Team (TCNOT). I provided key Computer Network Operations (CNO) support by performing validated threat CNO penetration testing and systems security analysis. TCNOT is the highest level of implementation of the CNO Team concept.

4. From 2008 to 2017, I also worked through a professional staffing company for several testing laboratories that tested electronic voting machines. These laboratories included Wyle Laboratories, which later turned into National Technical Systems (NTS), and Pro V&V. My duties were to perform security tests on vendor voting systems for certification. Certification was either to be obtained from the Election Assistance Commission (EAC) or a specific state's Secretary of State's requirements.

5. I have analyzed and verified Exhibit 1 "DominionIPnonprofitVOTINGresultstransfer [Autosaved].pptm" and reviewed Exhibit 2 "Dominion Voting Systems Petition for Approval of Electronic Voting Systems Democracy Suite 5.5-C and 5.5-CS." Both exhibits are attached. Based on my professional experience, I make the following observations.

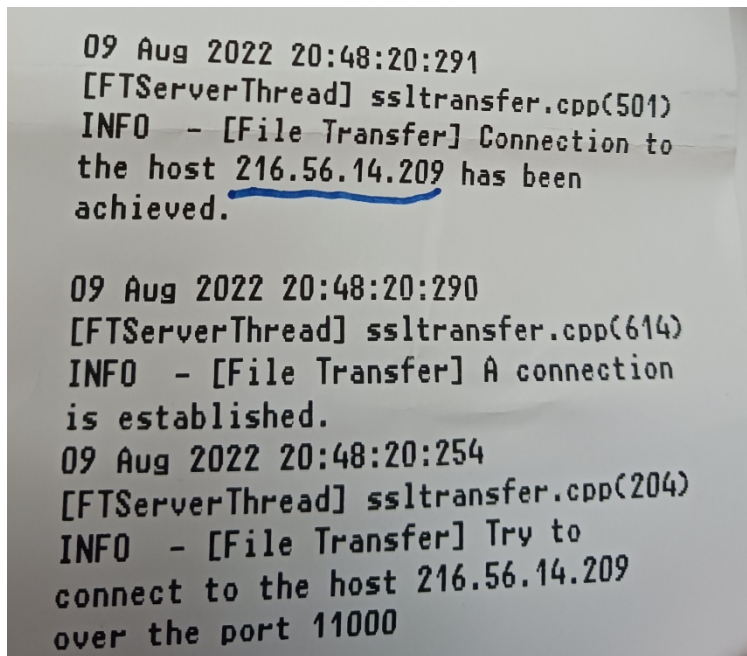
6. The host IP highlighted on slide 4 of Exhibit 1 (205.213.24.109) is what is known as a public IP address. This particular IP belongs to WiscNet.net which is headquartered in Madison, WI.



The Public IP address of a system is the IP address that is used to communicate outside the

organization's network. Public IP addresses are also referred to as "world facing" as they can be discovered, indexed, and accessed through on the Internet. A Public IP address has no security and is subjected to attack.¹

7. Slide 5 of Exhibit 1 shows yet another external connection from a different election.



This IP address (216.56.14.209) is

also registered to WiscNet.net. WiscNet is a private nonprofit company external to any of Wisconsin's election networks.

8. External connections pose several risks to electronic voting systems. One is to the election data in transit. It is susceptible to interception and or manipulation. Once data leaves a closed local network it has to make more "hops" to reach its destination. A hop is a computer networking term that refers to the number of routers that a packet (a portion of data) passes through from its source to its destination.² The more hops that data has to make the more exposed it is to attack. I traced the route, from several different locations, to each IP previously

¹ <https://www.geeksforgeeks.org/difference-between-private-and-public-ip-addresses/>

² <https://www.lifewire.com/what-are-hops-hop-counts-2625905>

identified. There were close to two dozen hops each before losing visibility. There were five to six hops alone just within the WiscNet.net domain.

9. Another risk from the external connection is to the actual voting system. The connection opens up the system to attack. It allows a path for a hacker to install malware or manipulate the system. The connections identified in Exhibit 1 can definitely allow for this type of malicious activity. The connections are established for secure file transfers, indicating that they use Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is standard Internet communications protocols that allow digital computers to communicate over long distances.³ TCP is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between the different devices over a network. Connection-oriented means that there is two-way communication. In other words, the system can both send and receive data. This capability to receive data is what puts the system at risk.

10. To communicate utilizing TCP/IP an application must also assign what's called a port. A port is a number that is assigned to user sessions and server applications in an IP network. The port is like the mailbox for the application. It is how it sends and receives data. The port shown for the file transfer connections in Exhibit 1 is "11000." This is not the standard port for any type of file transfer.⁴ In fact, port 11000 is known to be utilized by malware.⁵

11. Furthermore, the protocol or transport mechanism utilized on this port increases the danger and risk to the data and to the system. Exhibit 1 and 2 indicate the use of Secure Sockets

³ <https://www.britannica.com/technology/TCP-IP>

⁴ <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

⁵ <https://www.speedguide.net/port.php?port=11000>

Layer (SSL) by the electronic voting system. SSL is indicated in Exhibit 1 with the lines containing “ssltransfer.cpp.” The same log entry lines contain “[FTServerThread]” indicating further that this is more for transport security and not just for encryption. Exhibit 2, Appendix E lists OpenSSL for several components of the voting system. SSL as a transport mechanism is highly vulnerable and should not be used. Additionally, the version of OpenSSL listed in Exhibit 2 (1.0.2k) is an older version with multiple vulnerabilities. Even the latest versions of OpenSSL have been pulled by the application’s developers, stating “OpenSSL 3.0.6 and 1.1.1r are withdrawn. New releases will be created in due course.”⁶ This withdraw indicates what industry already knew: the SSL protocol is insecure and should not be used for the transport of data.

12. This weak two-way communication through an external connection is bad enough. Then add in the fact that the destination IP lies within the WiscNet domain and the risk and danger become a thousand times worse. The network and infrastructure maps within Exhibit 1 show WiscNet with a vast and dispersed network with multiple connecting sites. Each one of these connections could contain anywhere from ten to a hundred systems. Each system could be a possible point of attack. These connections indicate a high likelihood for attack with multiple attack vectors, and by connecting to WiscNet, the voting system has been connected to all of those sites, systems, external connections, users, and vulnerabilities

13. Slide 14 of Exhibit 1 list Verizon Pantech modem. Exhibit 2, page 3 states “Upgrade to modems with available 4G capabilities via the Verizon Private Network.” The existence of WiscNet IPs showing as connections on tabulator logs is proof that the data path is not traveling on a private network. Ms. Wolfe’s underlined statement on slide 11 of Exhibit 1 is incorrect. The results only partially travel over encrypted wireless networks. In Exhibit 2, page 14 under the

⁶ <https://www.openssl.org/> <https://www.openssl.org/news/vulnerabilities.html>

Modem Testing section it states "As part of Democracy Suite 5.5-C and 5.5-CS, the unofficial results data is encrypted, digitally signed, and then transmitted via a further encrypted virtual private network (VPN) hosted by Verizon Wireless." This is also a false and inaccurate statement. The Verizon Wireless is not a true Virtual Private Network (VPN). If it were a true VPN the connecting IP would be that of another Verizon device, not that of another company. Additionally, Appendix E of Exhibit 2, containing the EAC certification of Suite 5.5-C makes no mention of any cellular modem.

14. The lack of the modem being included as part of the Suite 5.5-C certification leads me to address other incorrect statements made in Ms. Wolfe's letter (slides 11-13 of Exhibit 1). She states "The modeming components of Democracy Suite 5.5-CS do not meet federal certification standards. However, the underlying voting system is federally certified." It appears the underlying system she refers to is Suite 5.5-C. Changing the USB port on the motherboard to accept a modem does indeed change the underlying voting system. The voting system has to send data across and through the device. Evidence of the motherboard being adapted to use the modem is in slide 3 of Exhibit 1, indicated by "externalportcontroller.cpp". This part of the code is controlling that USB connection on the motherboard. If Suite 5.5-C uses this modem or runs updated code to utilize the USB port it invalidates the certification of Democracy Suite 5.5-C; in other words, the underlying system is no longer 5.5-C, and it has not been federally certified. Additionally, in Exhibit 2, page 54 and 55 in the certification for Suite 5.5-C in the networking section it lists "NO" for modems and wireless. The only network connectivity allowed is Local Area Network use of TCP/IP which indicates LAN cabling and private IP space.

15. The petition for approval, Exhibit 2, consists of so many contradictions and inaccuracies concerning the Democracy Suite 5.5-C and 5.5-CS. I will clarify some of them. In the

Background section, page 2 states "5.5-CS being among them, the secondary system version lacks EAC certification, but is federally tested by an approved VSTL to comply with the 2005 Voluntary Voting Systems Guidelines (VVSG)." Further on it states that "The modeming components of Democracy Suite 5.5-CS do not meet federal certification standards." These statements conflict because the VVSG is the federal certification standard. The fact is the modems do not meet the federal certification standards. Volume 1 of VVSG 1.0 section 7.7.1 "Controlling Usage" states "In general, convenience is not a sufficiently compelling reason, on its own, to justify the inclusion of wireless communications in a voting system." The data being transmitted over these modems is always described as "unofficial election results," leading to the conclusion this transport action is for convenience.

16. Other concerns and inaccuracies are in the Modeming Functionality section, page 9 of Exhibit 2. One concern is that the section states "ICE and ICP2 communicate with the ImageCast Listener server." The EMS Server must have ImageCast Listener running as well as this is an ongoing function during an election. So, it is possible that the EMS has an external network connection. This is a concern as this listener has to run during the election, not just after the polls close. Another huge inaccuracy is in the portion of the section defining a "hardened and air gapped system." Yes, all non-necessary software and services should be removed, however, air gapped means "no network connectivity," period. It is not just restricting access to the internet.

17. Another very concerning contradiction is in Appendix F of Exhibit 2. Part 1 under Applicable VVSG Standard states the most recent version of the VVSG accepted by the EAC should be used. In Part 2 it states to use Volume 1 of the 2005 VVSG which is version 1.0. These are contradictory, since version 1.0 was approved in 2005 and two newer EAC-approved versions were available when DVS 5.5-CS was proposed (versions 1.1, in 2015, and 2.0, in

February, 2021). Also, the tests listed in this appendix do not seem to meet or comply with any VVSG version standard. They do not meet the most basic security requirements, let alone the rigorous standard of testing that should be used for a critical system.

18. Lastly, regardless of polls being closed or not the fact that a two-way, insecure, external connection is made makes the voting system highly vulnerable and susceptible to compromise. Hidden malware could already be residing on these voting systems. Given my education, experience as a security professional and my first-hand knowledge of testing nearly every vendor voting system product, it is my professional opinion that the voting systems listed in Exhibit 2 violate Wisconsin Statute 5.91(10). Section (10) states “It is suitably designed for the purpose used, of durable construction, and is usable safely, securely, efficiently and accurately in the conduct of elections and counting of ballots.” The use of the insecure SSL protocol in conjunction with a connection to an external entity by these voting systems is not of a suitable design for the purpose used. The system definitely is not safe and secure for use.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 29 day of October, 2022.


Clay U. Parikh

Exhibit 1



Dominion tabulator in Wisconsin, running firmware v5.5.6.5

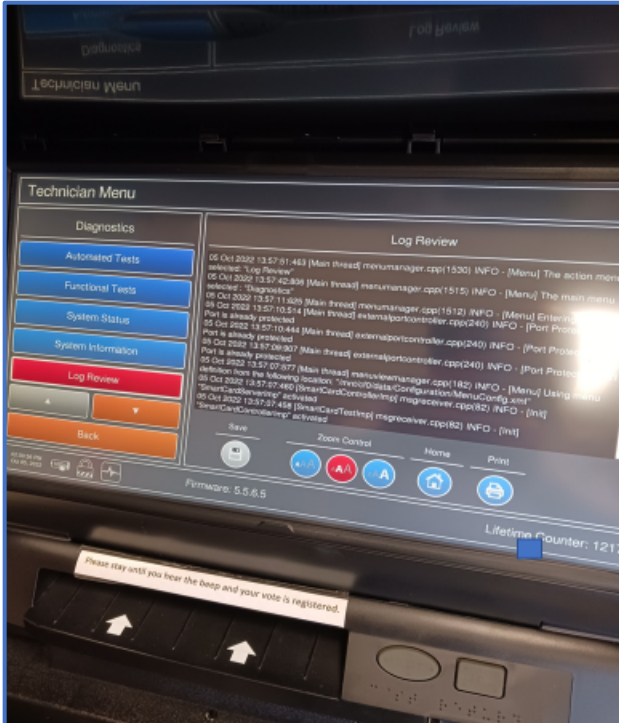
1



Technician Menu where election officials change the date and time for daylight savings time.

2

Exhibit 1



Log Review files, every Dominion tabulator has these. The can be printed out via the 3" wide paper tape, or, downloaded via the SLOG.txt file to a compact flash card.

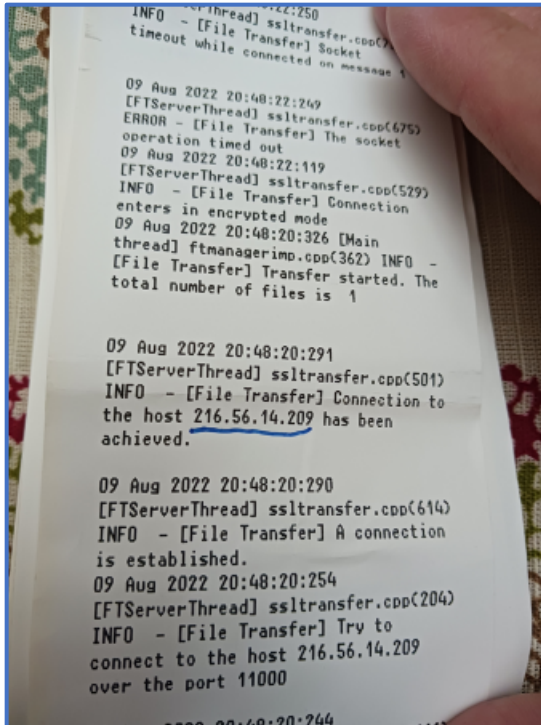
3

```
31 Mar 2021 13:41:04 INFO : [File Transfer] The socket is performing a reverse DNS lookup.
31 Mar 2021 13:41:04 INFO : [File Transfer] The socket has started establishing a connection.
31 Mar 2021 13:41:04 INFO : [File Transfer] Try to connect to the host 205.213.24.109 over the port 11000
31 Mar 2021 13:41:04 INFO : [File Transfer] A connection is established.
31 Mar 2021 13:41:04 INFO : [File Transfer] Connection to the host 205.213.24.109 has been achieved.
31 Mar 2021 13:41:04 INFO : [File Transfer] Transfer started. The total number of files is 1
31 Mar 2021 13:41:05 INFO : [File Transfer] Connection enters in encrypted mode
31 Mar 2021 13:41:05 WARN : [File Transfer] Already received tabulator -- Tabulator has already been received
31 Mar 2021 13:41:05 INFO : [File Transfer] Service request has been completed.
31 Mar 2021 13:41:05 INFO : [File Transfer] The socket is about to close (data may still be waiting to be written).
31 Mar 2021 13:41:05 INFO : [File Transfer] The socket is not connected.
31 Mar 2021 13:41:05 INFO : [File Transfer] Disconnected from the host 205.213.24.109
31 Mar 2021 13:41:05 INFO : [File Access] Writing to file: "/mnt/cf1/machinecontext_1_9.xml"
31 Mar 2021 13:41:05 INFO : [File Access] Writing to file: "/mnt/cf2/machinecontext_1_9.xml"
31 Mar 2021 13:41:07 INFO : [File Transfer] Stop monitoring of ppp0 link
31 Mar 2021 13:41:09 INFO : [Port Protection] Protect Administrator USB Port
```

Voting results of a test run before the April 2021 election being transferred to Wiscnet.net located in Madison, WI.

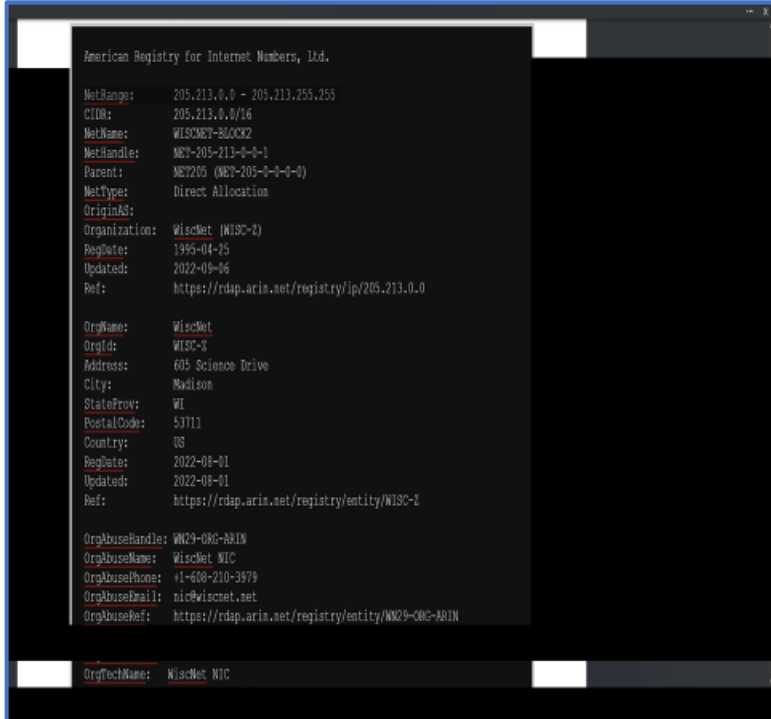
4

Exhibit 1



Voting results for the August 9th, 2022 primary are shown being transferred to Wiscnet.net in Madison, WI. Wiscnet.net is a nonprofit, private company. Dominion has stated in writing their voting results are transferred on secure Verizon cell phone lines. If true, the transfer should show going from the tabulator to the cell tower(s), to the county's EMS (election management system).


5



The IP address November 3rd, 2020 voting results were sent to were the nonprofit Wiscnet.net's IP address in Madison of 205.213.24.109.

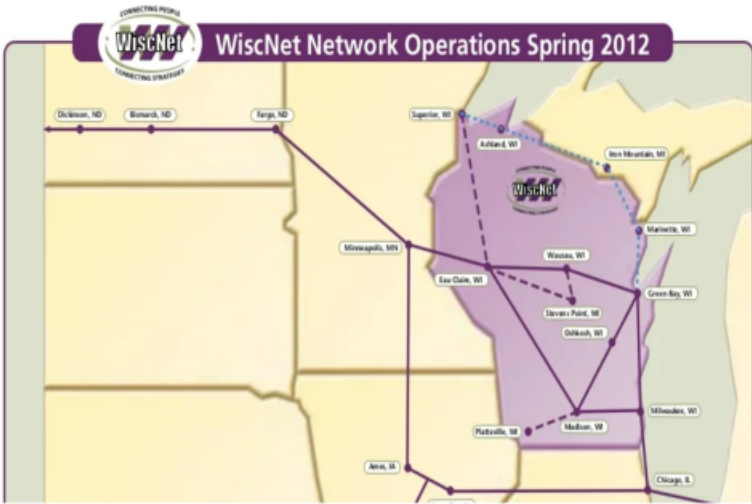
6

Exhibit 1

Decimal:	3627552465		
Hostname:	216.56.14.209		
ASN:	2381		
ISP:	WiscNet		
Services:	None detected		
Assignment:	Likely Static IP		
Country:	United States		
State/Region:	Wisconsin		Latitude: 44.936909 (44° 56' 12.87" N)
City:	Chippewa Falls		Longitude: -91.392929 (91° 23' 34.54" W)

This IP address, to which voting results were sent to, is the Eau Claire Technical College, part of the Wiscnet.net network. In the home district of State Senator Kathy Bernier.

7

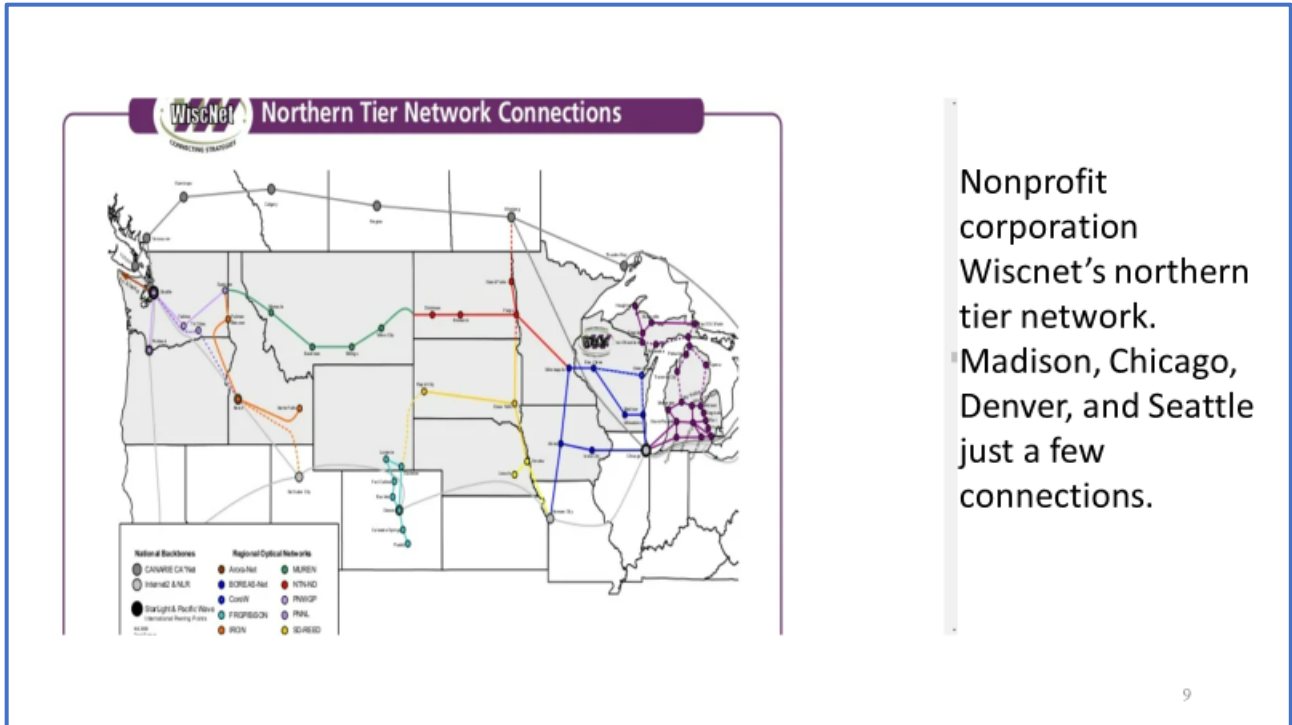


WiscNet Network Operations Spring 2012

Nonprofit corporation Wiscnet's local network connections.

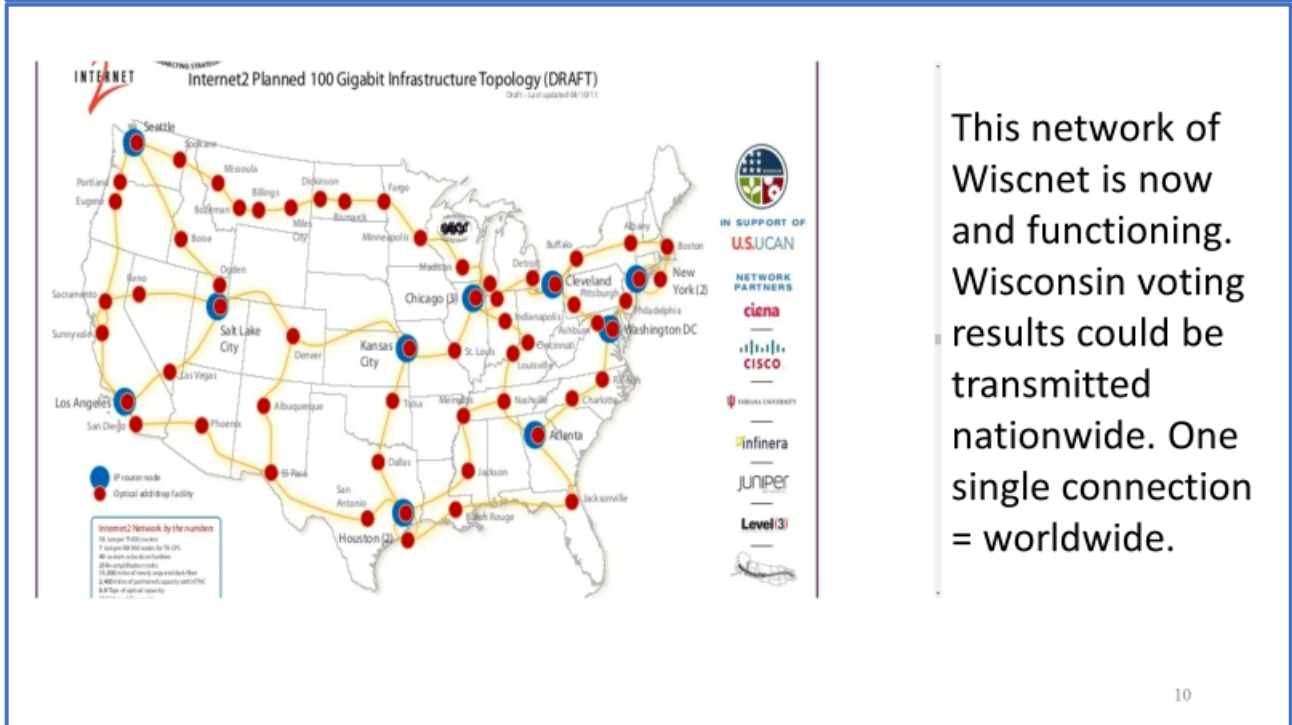
8

Exhibit 1



Nonprofit corporation Wiscnet's northern tier network. Madison, Chicago, Denver, and Seattle just a few connections.

9



This network of Wiscnet is now and functioning. Wisconsin voting results could be transmitted nationwide. One single connection = worldwide.

10

Exhibit 1

From Meagan Wolfe, Administrator of the Wisconsin Election Commission, letter of June 20, 2021:

“Democracy Suite 5.5-CS is a federally tested modification to the EAC certified Democracy Suite 5.5-C voting system. Democracy Suite 5.5-CS provides support for modeming of unofficial election results from an ImageCast Evolution or ImageCast Precinct 2 tabulator to a Secure File Transfer Protocol (SFTP) server through encrypted wireless telecommunications networks after the polls close on Election Day. The modeming components of Democracy Suite 5.5-CS do not meet federal certification standards. However, the underlying voting system is federally certified.”

Cont.- 1 of 3

11

Cont.-

“Updates introduced in this system version include:

- Election Management System client workstation upgraded to Windows 10.
- Upgrade to modems with available 4G capabilities via the Verizon Private Network.
- EMS and backend system components available in a standard and express configuration.
- Optional write-in report printed along with the results tapes on ICE and ICP2.
- Addition of ICX assistive voting devices with BMD and DRE configurations

The following paragraphs describe the design of the Democracy Suite 5.5-C and 5.5-CS hardware taken in part from DVS technical documentation.”

cont. 2 of 3

12

Cont. -
“ICE tabulators as part of Democracy Suite 5.5-CS also include external wireless and analog modems for the transmission of unofficial election results via an encrypted and secured 4G network hosted by Verizon Wireless or a standard telephone line.”

3 of 3

13



The Verizon modem stick used to transfer the voting data shown in the tapes in this slide presentation. It was placed into the tabulator after the results have been printed out on the 3” wide tape. Transfers typically take place 30 to 60 minutes after the polls close at 8pm in Wisconsin.

14

The Verizon modem stick is reprogrammed for every new election.

15

If the voting results transmitted are “unofficial” then the modems are not necessary at all. This would only give politicians, such as Robin Vos or Joe Biden, access to the voting results in time to stuff enough ballots to win their elections. Such as if there was a delay in reporting results in other, larger, municipalities. This is an opening to commit election fraud which must be closed.

Peter Bernegger www.wisconsinselectionjustice.org

16

Exhibit 1



Wisconsin Elections Commission

212 East Washington Avenue | Third Floor | P.O. Box 7984 | Madison, WI 53707-7984
{608} 266-8005 | elections@wi.gov | elections.wi.gov

DATE: For the June 2, 2021 Commission Meeting

TO: Members, Wisconsin Elections Commission

FROM: Meagan Wolfe
Administrator

Prepared and Presented by:
Robert Williams Cody Davies
Elections Specialist Elections Specialist

SUBJECT: Dominion Voting Systems
Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS

Introduction

Dominion Voting Systems (DVS) is requesting the Wisconsin Elections Commission (“WEC” or “Commission”) approve Democracy Suite 5.5-C and 5.5-CS voting systems for sale and use in the State of Wisconsin. The Government Accountability Board originally approved the Democracy Suite system, with Democracy Suite 4.14 D and 4.14 DS, on June 18, 2015 and this is an upgrade to that system. No electronic voting equipment may be offered for sale or utilized in Wisconsin unless first approved by the Commission based upon the requirements of Wis. Stat. § 5.91 (Appendix C). WEC has also adopted administrative rules detailing the approval process in Wis. Admin. Code Ch. EL 7 (Appendix D).

Recommendation

WEC staff is recommending approval of Democracy Suite 5.5-C and 5.5-CS for sale and use in Wisconsin. Detailed recommendations are listed on pages 24-26 following the analysis of functional and telecommunications testing performed by WEC staff.

Background

On September 3, 2020 WEC staff received an initial application for approval of Democracy Suite 5.5-CS. DVS submitted complete specifications for hardware, firmware, and software related to the voting system. In addition, DVS submitted technical manuals, documentation, and instruction materials necessary for the operation of Democracy Suite and 5.5-CS. Also included with the

Wisconsin Elections Commissioners

Ann S. Jacobs, chair | Marge Bostelmann | Julie M. Glancey | Dean Knudson | Robert Spindell | Mark L. Thomsen

Administrator
Meagan Wolfe

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 2 of 61

original application documentation was the testing report from the Voting Systems Testing Lab (VSTL) which conducted federal level testing for this system. Following conversations between WEC staff and representatives from DVS, the company also submitted an application for approval for Democracy Suite 5.5-C. This application was filed with all of the aforementioned supporting documentation, as well the system certification document from the federal Election Assistance Commission (EAC).

When an application is received for a system containing a telecommunications component for the transmission of unofficial election results, the voting system will contain a “base” system version which is federally tested and EAC certified, as well as a secondary system version which is identical to the “base” system except for the addition of telecommunications hardware. In such applications, Democracy Suite 5.5-C and 5.5-CS being among them, the secondary system version lacks EAC certification, but is federally tested by an approved VSTL to comply with the 2005 Voluntary Voting Systems Guidelines (VVSG). While Wisconsin state law (Wis. Stat. § 5.91) allows for state testing and Elections Commission certification of voting systems that lack federal EAC approval, it has been the practice of WEC to test both system versions where applicable. For the current test campaign, the Democracy Suite 5.5-C system has been granted EAC certification. Democracy Suite 5.5-CS lacks EAC certification but has undergone federal testing by a federally certified VSTL, Pro V&V, and Wisconsin specific functional testing by WEC staff.

Democracy Suite 5.5-CS is a federally tested modification to the EAC certified Democracy Suite 5.5-C voting system. Democracy Suite 5.5-CS provides support for modeming of unofficial election results from an ImageCast Evolution or ImageCast Precinct 2 tabulator to a Secure File Transfer Protocol (SFTP) server through encrypted wireless telecommunications networks after the polls close on Election Day. The modeming components of Democracy Suite 5.5-CS do not meet federal certification standards. However, the underlying voting system is federally certified.

System Overview

Democracy Suite 5.5-C is a federally tested, and EAC certified, paper based, digital scan voting system powered by the Democracy Suite software platform. It consists of seven major components:

- Election Management System (EMS) server.
- EMS client workstation (desktop and/or laptop computer).
- ImageCast X Ballot Marking Device (ICX BMD) an Americans with Disabilities Act (ADA) compliant vote capture device for polling place use.
- ImageCast X Direct Record Electronic voting device (ICX DRE) an ADA compliant vote capture device for polling place use.
- ImageCast Evolution (ICE), a polling place scanner and tabulator, which also meets ADA compliance requirements as a ballot marking device.
- ImageCast Precinct 2 (ICP2), a polling place scanner and tabulator.
- ImageCast Central (ICC), a high-speed scanner and tabulator for use in central count locations.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 3 of 61

Updates introduced in this system version include:

- Election Management System client workstation upgraded to Windows 10.
- Upgrade to modems with available 4G capabilities via the Verizon Private Network.
- EMS and backend system components available in a standard and express configuration.
- Optional write-in report printed along with the results tapes on ICE and ICP2.
- Addition of ICX assistive voting devices with BMD and DRE configurations

The following paragraphs describe the design of the Democracy Suite 5.5-C and 5.5-CS hardware taken in part from DVS technical documentation.

ImageCast Evolution

The ImageCast Evolution (ICE) is a digital scan paper ballot tabulator designed for use at the polling place. After the voter marks a paper ballot, their ballot is inserted into the unit for processing. The tabulator uses a high-resolution scanner to simultaneously image the front and back of the ballot. The resulting ballot images are then processed by proprietary mark recognition software, which identifies and evaluates marks made by the voter.

The system then tabulates any votes cast on each ballot before depositing the ballot into an integrated secured storage bin. The ballot images and election results are stored on a two separate, removable, compact flash memory devices. These compact flash drives operate in unison to maintain a detailed audit log of the tabulation events on election day. The cards maintain all ballot images and ballot manifests, a text document showing how the ICE counted each ballot cast on election day. The compact flash memory cards may be taken to the municipal clerk's office or county clerk's office where the election results may be uploaded into an election results management program or transferred to another memory device to facilitate storage. The ICE includes an internal thermal printer for the printing of the zero reports, log reports, and polling place totals upon the official closing of the polls. ICE tabulators as part of Democracy Suite 5.5-CS also include external wireless and analog modems for the transmission of unofficial election results via an encrypted and secured 4G network hosted by Verizon Wireless or a standard telephone line.



The ICE also serves as an ADA compliant ballot marking device, designed for use by voters who have visual or physical limitations or disabilities. Depending upon the configuration, voting either occurs on the primary tabulator screen or on an external monitor, both of which require using an assistive input device to make ballot selections. If the primary tabulator monitor is used for accessible voting, other ballot processing must be temporarily suspended until the accessible session has ended. When utilizing the external monitor, ballot processing on the tabulator can continue during the accessible voting session. An election inspector is required to begin the accessible voting session. Instructions that guide the voter through the process appear on the screen or can be accessed via the audio ballot function. Voters use an integrated tactile keypad, sip and puff device, or paddle selectors to navigate the ballot and make contest selections. Each button on the tactile keypad has both Braille and printed text labels designed to indicate function and a related shape to help the voter determine its use. In addition, voters may use headphones to access the audio ballot

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 4 of 61

function that provides a recording of the ballot instructions and lists candidates and options for each contest. A blank ballot is inserted into the tabulator ballot slot prior to making selections when the primary screen is used. For locations with an external monitor, voters make ballot selections and place the blank ballot in the tabulator ballot slot at the end of the process. In either method, the ballot is marked according to the voter's selections and automatically returned for review. Once the voter has reviewed their ballot, it is reinserted into the tabulator for processing.

ImageCast Precinct 2

The ImageCast Precinct 2 (ICP2) is a digital scan paper ballot tabulator designed for use at the polling place. After the voter marks a paper ballot, their ballot is inserted into the unit for processing. The tabulator uses a high-resolution scanner to simultaneously image the front and back of the ballot. The resulting ballot images are then processed by proprietary mark recognition software, which identifies and evaluates marks made by the voter. The system then tabulates any votes cast on each ballot before depositing the ballot into an integrated secured storage bin.



The ballot images and election results are stored on two separate, removable, SD memory devices. These SD drives operate in unison to maintain a detailed audit log of the tabulation events on election day. The cards maintain all ballot images and ballot manifests, a text document showing how the ICP2 counted each ballot cast on election day. The SD memory cards may be taken to the municipal clerk's office or county clerk's office where the election results may be uploaded into an election results management program or transferred to another memory device to facilitate storage. The ICP2 includes an internal thermal printer for the printing of the zero reports, log reports, and polling place totals upon the official closing of the polls. ICP2 tabulators as part of Democracy Suite 5.5-CS also include external wireless and analog modems for the transmission of unofficial election results via an encrypted and secured 4G network hosted by Verizon Wireless or a standard telephone line. The ICP2 does not include any accessible voting functionality and would need to be paired with another ADA-compliant component from the system to meet the accessible voting requirements.

ImageCast Evolution and ImageCast Precinct 2 Voter Information Screens: The ICE and ICP2 feature a touchscreen display to provide feedback to the voter regarding the disposition of any ballot inserted into the machine. The screens are designed to alert voters to errors on their ballot. The tabulators will, depending on the situation, provide details about the error, identify the specific contests where the errors occurred, allow the ballot to be returned to the voter, and provide the option for the voter to cast the ballot with errors on it. Information below gives examples of the notifications provided to voters in specific situations, with approved Commission language, where applicable. Images of these screens can be found in Appendix B.

- **Overvote Notification:** If the ballot contains an overvote, a message appears that identifies the contest or contests with overvotes. The message also tells the voter that these votes will not count. The language displayed in this notification reflects language requirements as approved by the Commission, which states:

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 5 of 61

- “You have filled in too many ovals in 2 contests. These votes will not count.”
- “To correct your ballot press RETURN and ask for a new ballot.”
- “To cast your ballot with votes that will not count, press CAST.”

The voter has the option to return the ballot for review or cast the ballot. If there are multiple errors the voter is able to review them all. Instructions above the “Return” button direct the voter to press “Return” if they wish to correct their ballot. The voter is also instructed to ask for a new ballot. Instructions direct the voter to press “Cast” if they wish to submit their ballot with votes that will not count.

- **Crossover Vote Notification:** If a ballot is inserted with votes in more than one party’s primary and no selection has been made in the party preference section of the ballot, a message appears that informs the voter that their ballot contains crossover votes. As in the notification for an overvote, the language displayed in this notification reflects language requirements as approved by the Commission, which states:
 - “Cross Over Votes Detected. You selected candidates from different parties. If you cast the ballot as marked, no votes in any partisan contest will count.”
 - “To change your ballot and make selections in only one party, press RETURN and ask for a new ballot.”
 - “To cast your ballot with cross over votes, press CAST. Your votes in partisan contests will not be counted.”

The voter has the ability to return the ballot for review or cast the ballot with crossover votes. Instructions direct the voter to press “Return” if they wish to correct their ballot to reflect their party preference or vote a new ballot. The voter is instructed to ask for a new ballot. The voter does have the option to cast the crossover-voted ballot. The crossover vote warning screen is programmed to notify the voter that no votes in any partisan contest will be counted should the crossover-voted ballot be cast.

- **Blank Ballot Notification:** If the ballot contains no votes, a message appears stating that the ballot is blank. The voter is instructed to press “Return” to correct their ballot and see a poll worker for help. The voter is instructed to press “Cast Blank Ballot” to submit their ballot without any selections.
- **Error Scanning Ballot:** If a ballot is inserted incorrectly, the ICE and ICP2 will return the ballot to the voter and advise that the voter reinsert the ballot into the tabulator. The ICE and ICP2 do not allow the voter to cast the ballot without resolving the issue and, if the issue persists, the voter is instructed to contact a poll worker for assistance.
- **Ballot Jam:** This message will be displayed if a ballot becomes jammed during the scanning process. The voter is informed that the tabulator has jammed and that they should contact a poll worker. Voters are also informed of the disposition of their ballot. If the jam occurred prior to tabulation, the screen tells the voter their ballot was not counted.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 6 of 61

This system may also be programmed, at the request of the municipality, to automatically reject all ballots with overvotes or crossover votes without the option for override, which requires the voter to correct the error by remaking his or her ballot. This ensures that voters do not mistakenly process a ballot on which a vote for one candidate or all candidates will not count. In such municipalities, absentee ballots must be remade by election inspectors without the improperly voted contests following the appropriate procedures as explained in state law and the election day manual.

The ICE and ICP2 are also capable of producing a results report showing all candidates with write-in votes. This report captures an image of what is written on the write-in vote line if the oval was darkened. Presently, the write-in report is not approved for use. Election inspectors, instead, review ballots by hand, searching for write-in votes. This certification application is not seeking approval for the utilization of the write-in report. Per DVS, the system was developed anticipating the possibility of future legislation allowing for its use.

ImageCast Central

The ImageCast Central (ICC) is a high-speed, digital scan ballot tabulator designed for use by election officials at a central count facility. The ICC is capable of scanning ballots of various sizes. It uses a commercial off the shelf printer to read the front and back of each ballot, evaluate the result, and maintain continuous scanning and tabulating. Election officials use a touchscreen display to program these features of the ICC. While processing ballots, the ICC displays a continuous ballot scan speed indicator. Average scan speed with a 17-inch ballot approximately 100 ballots per minute. Reports can be printed from a separate connected printer. The ICC saves voter selections and ballot images to a USB flash drive for processing with the Election Management System.



Reading Ballots: The ICE, ICP2, and ICC use proprietary software to identify properly marked votes on a hand-marked ballot. Ballots used in conjunction with this system are designed with an oval next to the candidate name or write-in area. The machine uses coordinates determined by the timing marks laid out and printed on the border of the optical scan ballot to determine which contest and candidate each filled-in oval corresponds with. Tabulators do not read the actual candidate name printed next to the oval to determine voter intent. Voting equipment programming is responsible for determining the correlation between the filled-in oval and the candidate name. This programming is completed prior to the election with a statutorily required public test of the equipment included as both a way to confirm the accuracy of the programming and an added election transparency measure.

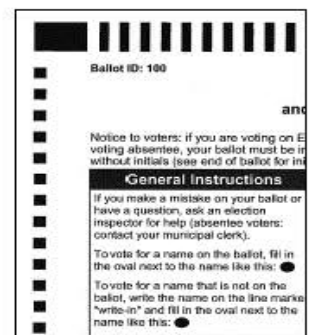


Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 7 of 61

As the tabulator scans the ballot to determine the choices made by a voter, a digital image of both sides of the ballot is simultaneously captured by the machine. These ballot images are saved as part of the election audit trail and accessible by either the county clerk or the vendor. Accompanying each ballot image is information on how the ballot was adjudicated by the tabulator. These ballot manifestations inform election officials how each vote on every ballot was counted by the tabulator, allowing officials to know which candidates received votes on any given ballot in the event of an audit or recount.

ICX BMD and DRE

ICX is an accessible touchscreen device primarily designed for use by voters who have visual, auditory, or physical limitations or disabilities, which is offered in either a ballot marking device (BMD) or direct record electronic (DRE) configuration. The ICX uses unmodified, commercially available off the shelf hardware such as touchscreen displays and desktop printers, combined with personal assistive devices, and specially developed software to form a voting device. ICX BMD has no tabulation feature and the ballots marked using this system cannot be processed on the ICE and ICP 2 precinct tabulators.



ICX DRE voting devices utilize the same user interface as the BMD counterpart. Instead of a ballot being printed on a standard piece of ballot stock, ballots are printed on a Voter Verified Paper Audit Trail (VVPAT) printer. The VVPAT serves as the official ballot for the voters using this device to cast their ballot and the ICX DRE is capable of tabulating ballots cast on the device.

An activation card is necessary to begin a voting session. Depending on the type of activation card used, an election inspector may need to assist the voter to access the correct ballot style for the election. Another activation card option allows a voter specific card to be created that corresponds to a unique ballot style. Poll worker activation cards can be used an unlimited number of times. Voter activation cards must be reprogrammed after every use. It is also possible to set the voter activation cards to expire after a certain amount of time if not used. This way, activation cards cannot be taken out of the polling place and used at a later time or date. Any attempt at doing so after the programming had expired would result in a prompt displayed on the ICX directing the voter to insert an appropriately programmed activation card in order to access the correct ballot style.

Once the correct ballot style has been selected, either by an election inspector or by the voter using a pre-programmed voter activation card, the voter is left to navigate the ballot and cast their votes privately. Voters have the option to use the touchscreen, a sip and puff device, paddle selectors, or an integrated tactile keypad to navigate the ballot and make their selections. Instructions that guide the voter through the process appear on the screen or can be accessed via the audio ballot function. Voters have the option to adjust the text display contrast and text size to suit their preferences. Each button on the tactile keypad has both Braille and printed text labels designed to indicate function and a related shape to help the voter determine its use. Voters may also use headphones to access the

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 8 of 61

audio ballot function that provides a recording of the ballot instructions and lists candidates and options for each contest. The volume of the audio can be adjusted by voters.

In both BMD and DRE configurations, the ICX provides a ballot summary screen on which voters can review their selections before the ballot is printed. Once a voter confirms their selections, those selections are sent to an attached printer which utilizes either blank ballot stock or a VVPAT paper printer to produce a marked ballot containing all of the voter's selections. When the ballot is printed, both types of ICX ballots differ in format from that of the hand marked optical scan ballots.

The contests on the BMD ballot, as well as voter selections, are listed in columns and rows, but there are no ovals or timing marks on the ballot. A QR code is present on the final printed ballot. However, the QR code would not be utilized due to the fact that neither the ICE nor the ICP2 are programmed to tabulate ICX BMD ballots. After the voter completes the process, the paper ballot is the only record of the voting selections made. ICX BMD does not save any vote or ballot information to its internal memory. Ballots marked using ICX BMD can be deposited into a secured ballot box to be hand tabulated by election inspectors after the polls have closed. As there is no option to electronically tabulate ICX BMD ballots, they must be hand counted.

Voter selections marked on the ICX DRE (pictured, right) are presented to the voter on a VVPAT paper printer, as well as saved internally for tabulation after the close of polls. This style of printer uses rolls of paper that are spooled inside of a locked and secured vertical printing mechanism. Once the voter confirms their selections on the summary screen, those selections are sent to the attached VVPAT printer, which prints the voter's choices, and advances the paper roll so the voter has the opportunity to physically review the paper artifact on to which their votes are marked. Until the ballot is printed, the window through which voters view their selections remains opaque. When a ballot is advanced into the window for review, an internal light illuminates the ballot, and the window becomes transparent. Voters are given a final choice to accept the ballot as presented on the VVPAT, or to reject the ballot and vote a new one. When the voter chooses to accept the ballot, the paper roll advances so that the ballot is no longer viewable. At this time, the contests and candidates selected are also saved to the internal USB memory device for later tabulation. Both the touchscreen and printer then return to their original state, ready for the next voter. After the polls have closed on election day, election inspectors close the polls on the ICX DRE much as they would on an optical scan tabulator. A results tape is generated by the VVPAT printer showing contest and candidate totals. Results are also saved to the internal USB memory device for transfer to the election management system.



When voting on the ICX BMD or DRE in a Partisan Primary or Presidential Preference Primary election, voters must make a party preference selection before viewing contests so that crossover votes cannot occur. Once the voter makes their party preference selection, they will see candidates from only that party for all contests. Should the voter wish to see candidates in another party, they would be required to navigate back to the beginning screen and make a different party preference

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 9 of 61

selection. On primary ballots that contain both partisan and nonpartisan contests, there is also a nonpartisan option on the party preference selection screen. When a voter makes this selection, the ICX automatically transitions the voter to the nonpartisan offices on the ballot.

Modeming Functionality

Democracy Suite 5.5-CS provides support for modeming of unofficial election results from an ICE or ICP2 to a Secure File Transfer Protocol (SFTP) server using the ImageCast Listener server software, located in the offices of the county clerk. Transmissions are sent through a secured and encrypted wireless telecommunications network or analog phone network. The external wireless modems used with the ICE and ICP2 communicate with the ImageCast Listener server via a 4g connection hosted on the Verizon Private Network to transmit unofficial election night results as an encrypted data packet to a secure server at a central office location, such as the county clerk's office.

The modem function on the ICE and ICP2 may only be used after an election inspector has closed the polls, utilized a multi-factor authentication token, and entered a password to access the poll worker menu. Following the printing of the results tape, election inspectors connect the external modem and select on the poll worker menu of the tabulator the option to transmit results to the county. After this option is selected, the tabulator screen provides informational prompts to the election inspectors related to where in the transmission process the machine is at any given time. The encrypted data packet comprised of the unofficial election results is received in the county office by the ImageCast Listener server and EMS server software.

In the office of the County Clerk, a firewall provides a buffer between the network segment, where the election server is located, and other internal networks which utilize separate servers. The data that is transmitted is encrypted and it is digitally signed. The network is configured to only allow valid connections with the correct encryption key to connect to the SFTP server. The firewall further restricts the flow and connectivity of traffic. Only after the system determines that an incoming data packet contains the correct encryption key, the information is passed through the SFTP server and on to the Election Management System (EMS) workstation. Any transmission received must contain the correct and matching decryption key. If the decryption key does not match that of the incoming transmission, or if some aspect of the hardware sending the transmission cannot be authenticated by the server and EMS workstation software, the transmission is rejected.

The EMS is required to be deployed on a hardened and air gapped system pursuant to the 2005 Voluntary Voting System Guidelines, meaning that all software that is not essential to the proper functioning of the EMS is removed from the computer where the EMS is installed. This procedure is designed to increase the security of the system through the elimination of applications that may provide "back door" access to the system. Access to the internet is also restricted and the EMS provides an audit log of all system actions and connection attempts that can be used to verify unauthorized access to the system while unofficial election results are being transmitted after the close of polls.

EMS servers in both the standard and express configuration as part of Democracy Suite 5.5-CS support the transmission of results via wireless or analog modems utilizing a standard phone line connection. During this test campaign, WEC staff successfully transmitted results in each county

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 10 of 61

listed below using wireless or analog modems in each municipality. During this test campaign, the strength of service ranged from zero bars (lowest indicator level is zero) to five bars (highest indicator level). In locations where signal strength is an issue, there is an optional booster antenna available that connects directly to the modem to increase wireless capabilities.

WEC staff conducted testing of Democracy Suite 5.5-CS in three counties: Washington, Green, and Walworth, between April 26 and 28, 2021. As a result of technical issues in the original modem tests, a follow up round of testing was conducted in Washington County on May 14, 2021. In consultation with each county clerk, WEC staff selected three municipalities in each county to serve as locations for testing.¹ The municipalities were selected in part because of the strength of the wireless networks in the community, or lack thereof, and the municipal clerk's willingness to host the test team. Results of these tests can be found beginning on page 14 of this report.

At its May 21, 2013, meeting, pursuant to authority granted in Wis. Stat. § 5.91 and Wis. Admin. Code Ch. EL 7, the Government Accountability Board adopted testing procedures and standards pertaining to the modeming and communication functionality of voting systems that have not received EAC certification. The standards were based upon the analysis and findings outlined in a staff memorandum and detailed in the *Voting Systems Standards, Testing Protocols and Procedures Pertaining to the Use of Communication Devices in Wisconsin*, which are attached as Appendix F. These rules apply to non-EAC certified voting systems, where the underlying voting system received EAC certification to either the 2002 Voting System Standards (VSS) or 2005 VVSG, but any additional modeming component does not meet the 2005 VVSG.

Functional Testing

As required by Wis. Admin. Code EL § 7.02(1), WEC staff conducted three mock elections with each component of Democracy Suite 5.5-C and 5.5-CS to ensure the voting system conforms to all Wisconsin requirements as laid out in Wis. Stat. § 5.91. These mock elections included: A partisan primary with a special nonpartisan school board election, a general election with both a presidential and special gubernatorial contest, and a presidential preference primary combined with a nonpartisan election with a partisan special election for Representative to the Assembly.

WEC staff designed a test script of roughly 6,200 ballot placements on 1,800 ballots using various configurations of votes over the three mock elections to verify the accuracy and functional capabilities of Democracy Suite 5.5-C and 5.5-CS. Using blank test ballots supplied by DVS, WEC staff appropriately marked votes for contests and candidates as designated on a test script spreadsheet developed for the current test campaign. For each mock election, 400 ballots were marked for tabulation. Hand marking was utilized for 300 paper ballots fed through the ICE, ICP2, and ICC. The remaining 100 ballots per mock election were marked using the accessible components of the system, the ICE Tabulator BMD and ICX BMD. These devices were tested by marking 150 ballots per BMD type across the three mock elections for a total of 300 BMD ballots marked. This total included 50 ballots per BMD for each mock election.

¹ Washington County: Town of Polk, Village of Jackson, Town of Trenton
Green County: Town of Monroe, Village of Browntown, City of Monroe
Walworth County: Village of Fontana, City of Lake Geneva, City of Elkhorn

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 11 of 61

The paper ballots marked, as well as the votes captured by the ICE Tabulator BMD, ICX BMD, as well as the ICX DRE were verified by WEC staff before being scanned and counted by the ICE, ICP2, and ICC. WEC staff ensured that the results produced by the three pieces of equipment were accurate and reconciled with the test script prior to transitioning to testing the next mock election type. A small number of results anomalies, explained below, were investigated and resolved in real time.

Votes were recorded on test ballots in a variety of configurations in all contests to ensure that the programming of the tabulation equipment was compatible with Wisconsin election law, and that the equipment processed ballot markings in accordance with statutory requirements. Ballots were purposefully marked with overvoted contests and the equipment was able to consistently identify those scenarios and inform the voter about the specific contest, or contests, that were problematic. Ballots for both the Partisan Primary and Presidential Preference mock elections were also marked with votes that crossed party lines and, in each instance, the machines were able to identify those crossover votes and display the warning screen to the voter.

Two different ballot styles were used for each mock election and one ballot style in each election had a special election contest included on the ballot. This inclusion was used to determine if the equipment could be programmed to accommodate multiple election definitions on the same ballot style and produce accurate results. The equipment was found to have accurately tabulated votes and correctly reflected Wisconsin election law in the programming on both ballot styles.

Programming on the Democracy Suite 5.5-C and 5.5-CS tabulation equipment includes a default level at which a marked oval is read as a good vote. Any mark in an oval which occupies more than 12% of the total space of the oval is counted by the tabulation equipment as a good vote. Marks that occupy less than 12% of the oval are read by the equipment as ambiguous marks. Ballots with marks not meeting this minimum threshold would be returned to the voter or election inspector for having selections not completely discernable by the tabulator. This 12% minimum mark threshold is adjustable to allow for a higher or lower percentage of the oval that must be filled in to be considered a good mark by the tabulation equipment. In an effort to maintain statewide uniformity on what will count as a good vote in municipalities using this system, if certified, the 12% threshold is included in staff recommendations beginning on page 24.

The test scripts used for this campaign were also designed to determine what constitutes a readable mark by each piece of tabulation equipment included in this system. A subset of ballots in the test deck were marked using “special marks.” The ballots with special marks were processed by the tabulation equipment. WEC staff reviewed the results to determine which of the special marks were read by the tabulation machines. The chart below illustrates actual marks from test deck ballots that were successfully read and counted as “good marks” by the ICE, ICP2 and ICC.

In each is don

<input checked="" type="radio"/> Turanga Leela	<input checked="" type="radio"/> William Adama	<input type="radio"/> James T. Kirk	<input type="radio"/> Roger Waters	<input checked="" type="radio"/> Delta Walker
<input type="radio"/> Phillip J. Fry	<input type="radio"/> Tom Zerek	<input checked="" type="radio"/> Harry Mudd	<input checked="" type="radio"/> David Gilmour	<input type="radio"/> Susannah Dean
<input type="radio"/> Uninstructed	<input type="radio"/> Uninstructed	<input type="radio"/> Uninstructed	<input type="radio"/>	<input type="radio"/>

s

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 12 of 61

devices that do not adhere to vendor recommendations. All three pieces of equipment were able to correctly read marks in pencil, black pen, blue pen, as well as marks made with fine point felt tip markers, which is the marking pen recommended for use by DVS. Ballots marked with red ink, however, required additional analysis during testing due to the fact that they were initially processed inconsistently on the tabulation equipment. A more detailed description of this issue can be found in the Testing Anomalies section of this report.

The test scripts also included ballots folded to simulate hastily folded absentee ballots. Folded ballots were able to be processed on the ICE, ICP2, and ICC. Folds through the oval and write-in area on the ballots did not create any issues in testing. As tested, and recommended for certification, the equipment reviews only the oval on any ballot when scanning for marks. There is always the possibility, however, for ballots with heavy folds directly through the oval to create what is best described as a false positive vote.

Democracy Suite 5.5-C and 5.5-CS testing also included ballots with both slight and severe tears. While all three pieces of equipment successfully processed slightly torn ballots without incident, anything other than a slight tear was inconsistently processed by the equipment. In some instances, the ballot would be returned by the tabulator, only to be accepted when run through again. This is especially true if there is a tear in a ballot which runs through one of the timing marks. If the tabulator cannot clearly scan all timing marks on the ballot, any such ballots will be returned to the voter or election inspector for review. Ballots with large tears cause a jam in both the ImageCast Central and will likely not be processed by the ImageCast Evolution or ICP2.

Blank ballots were also included to determine how each of the three different tabulators would treat these ballots. The ICE and ICP2 were able to identify blank ballots and provide a warning message to the voter that indicated the ballot was blank and provide options to return the ballot or cast it as is. This functionality was also tested on the ICC, which successfully identified blank ballots in the reports and adjudication software.

Write-in votes tabulated by the ICE and ICP2 are scanned and read in the same manner as ballots for named candidates. In order for the tabulation equipment to recognize a write-in vote, voters must fill in the oval next to the appropriate write-in line. If a voter writes in the name of a candidate, but fails to mark the oval, the tabulation equipment will not recognize a valid mark. An optional write-in report can be printed at the same time as the results tape after the close of polls. This report only shows write-in votes for which the oval has been marked. For this reason, election inspectors should not rely upon the write-in report to provide a complete picture of the write-in totals, instead conducting a hand tally of all write-in votes after the close of polls. After the processing of a ballot containing write-in votes, and depending on the ballot box used, these ballots may be diverted into a separate write-in bin. Since the write-in ballot bin has a smaller capacity than the general ballot bin, election inspectors may be required to move the contents of the write-in bin to the larger ballot bin at some point on election day.

Testing Anomalies

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 13 of 61

Throughout the in-office testing process, staff encountered minor anomalies that, while explainable and which were ultimately resolved, warrant mention. It is also important to note that none of the anomalies referenced in the following paragraphs affected the outcome of the testing procedures in any way and that there was no indication of any issue with the functionality of the equipment being tested. After identifying and addressing the issues, which are further explained below, the test decks from all three mock elections reconciled appropriately without further complications.

Prior to tabulating the test deck for each election on the full suite of tabulation equipment, staff began each round of testing by first proofing the test ballots on the ImageCast Central count scanner to ensure that the ballots were marked in accordance with the test script. When proofing the test ballots for the partisan primary election, the results were consistently off in several contests. Upon further review, the cause of this issue was determined to be two ballots included in the test deck on which contests were marked with red ink. This issue was also present in the test decks for the general election and presidential preference primary, which are similarly designed to include ballots marked with red ink.

After analysis, staff determined that the ICC central count tabulator being used to proof the test decks in each election required that an optional parameter be selected to correctly read red ink. When the central count scanner settings were changed to include reviewing ballots for red ink, all ballots were appropriately tabulated by this specific tabulator. There were, however, instances where ballots marked in red ink were initially returned by the ICE and ICP2. Upon reinserting the ballots, they were ultimately accepted. The reason for this is the system capabilities and the nature of the ink used. Ballots marked with red ink that is considered to be “true red” may experience issues being processed on the tabulation equipment. Some types of red ink actually contain trace amounts of black ink. Ballots marked with this type of red ink should have no issue being processed by the tabulators. The issue of ballots marked with red ink is something that is directly addressed by DVS. Instructions are included on ballots for the currently certified Democracy Suite system, Democracy Suite 4.14, stating that red ink should not be used. It is important to note that, while voters are instructed to mark their ballots with a black felt tip marker, all pieces of tabulation equipment tested as part of Democracy Suite 5.5-C and 5.5-CS were ultimately capable of appropriately identifying ovals marked in red ink.

In a separate situation, staff was initially unable to reconcile the results of the presidential preference primary election. After multiple reviews of the results from each tabulating device and the test matrix for that election, it was determined that two ballots had been inadvertently duplicated during the preparation process. As a result, ballot number 198 and 199 were included twice in the pool of test ballots. To rectify the situation, staff located the two duplicate ballots, removed them, and retabulated the test deck on the entire suite of equipment. After this subsequent round of tabulation, the machine results and the test matrix reconciled perfectly.

Another anomaly was discovered that was specific to the ICX DRE, which is a piece of equipment that records voter’s choices on receipt style VVPAT tape. When staff attempted to reconcile the elections marked on the ICX DRE, each of which had a unique test matrix specific to this piece of equipment, the final results did not match the test matrix. After an extensive ballot-by-ballot review of the VVPATs for each election, staff was able to determine certain ballots had been marked incorrectly during the initial phase of testing. After further reviewing the test matrix and

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 14 of 61

determining which ballots had been mismarked during the testing protocol, and identifying and accounting for these mismarked ballots, the results for all three elections were reconciled successfully.

Anomalies such as these are common and expected during test campaigns. While the ballots in the test decks for the mock elections are proofed for errors after being marked, there is always the potential for a mismarked ballot, or duplicate ballots, to be inadvertently missed during review. When the results of an election do not match the test matrix, staff goes to great lengths to identify the root cause of the discrepancy, which can include tabulating the same test ballots multiple times and reviewing each of the ballots for a particular election until the anomaly is identified and resolved.

To reiterate, none of the anomalies encountered during this test campaign affected the ultimate outcome of the certification tests in any way. All three mock elections tabulated on the main suite of equipment and three additional mock elections specific to the ICX DRE reconciled, as required. Testing results and staff observation of the system indicate that Democracy Suite 5.5-C and 5.5-CS consistently identifies and tabulates correctly marked ballots in a uniform fashion.

Modem Testing

WEC staff conducted functional testing of Democracy Suite 5.5-C and 5.5-CS in Washington, Green, and Walworth counties in accordance with the *Voting Systems Standards, Testing Protocols and Procedures Pertaining to the Use of Communication Devices in Wisconsin*. A four-person team of WEC staff conducted this testing campaign April 26-29, 2021 with a second round of testing in Washington County on May 14, 2021. Four representatives from DVS were on hand in each county to provide technical support. DVS provided three (3) ICE and ICP2 units in each county, each equipped with a Verizon wireless modem. Also provided by DVS as part of testing was a portable EMS environment, which included an SFTP client, firewall, etc.

In each location, DVS set up the portable environment in the county office to receive test election results from each municipal testing location. In each municipal location, WEC staff inserted a pre-marked package of 10 test ballots through both the ICE and ICP2 to create an election results packet to transmit to the county office. Both tabulators were also tested to ensure that two separate server configurations at the county were able to receive results. A WEC staff member was present at the county office to observe how the portable EMS environment handled the transmissions. As two tabulators were being tested in each location using two server configurations (Standard and Express) at the county office, staff effectively conducted four complete tests of the telecommunications capabilities of this system in each municipality.

As in previous test campaigns, staff tested both wireless and analog (wired) modems to ensure that results packets were capable of transmitting to the county on either configuration. As part of Democracy Suite 5.5-C and 5.5-CS, the unofficial results data is encrypted, digitally signed, and then transmitted via a further encrypted virtual private network (VPN) hosted by Verizon Wireless. Without the correct encryption key, the incoming data is prevented from reaching the EMS workstation.

An optional component of this system was also tested in addition to the ICE and ICP2. The Results Transfer Manager (RTM) is a standalone application used in conjunction with the Election

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 15 of 61

Management System (EMS) that allows for the secure transmission of election results from a remote location to a central location. This method of results transmission is used in lieu of modeming directly from a tabulator and allows the media cartridge from the tabulator to be plugged into a secure device, from which the results from multiple tabulators/devices can all be transmitted to the EMS at the county at the same time. This component performed in accordance with testing standards and there were no issues with the results transmission process.

Washington County

On April 26, 2021, WEC staff conducted tests on the Democracy Suite 5.5-C and 5.5-CS modem component in three municipalities in Washington County: Village of Jackson, Town of Trenton, and Town of Polk. DVS conducted pre-testing of the Democracy Suite 5.5-C and 5.5-CS wireless modem components in Washington County prior to WEC testing. An ICE and ICP2, each equipped with Verizon modems, were tested in all three municipalities. A test script was used to ensure that each tabulator conforms to the communications device standards and that each was able to transmit accurate election results data to the Election Management System.

The first round of modem testing in Washington County was not successful. While staff was able to intermittently transmit results to the county office, none of the sites were able to fully complete testing and one municipality, the Town of Trenton, was not able to transmit a single results packet at any point during this test. Following this series of issues, DVS staff were able to determine that the root cause of the connectivity issue was the prepaid SIM cards being used for testing. The prepaid cards were not correctly set up with the proper IMEI number for each device and, as such, the server did not allow transmissions from the modems utilizing those cards. As this issue was not considered to be a fault of the system itself, WEC staff coordinated a second round of testing in Washington County on May 14, 2021, during which the modems all performed to adequate standards.

Washington County (Wireless)					
		ICE		ICP2	
		Standard	Express	Standard	Express
Village of Jackson					
Initial Transmission		10 of 10	10 of 10	10 of 10	10 of 10
Load Test		12 of 12	11 of 11	14 of 14	9 of 9
Town of Polk					
Initial Transmission		10 of 10	10 of 10	10 of 10	10 of 10
Load Test		9 of 9	7 of 7	11 of 11	10 of 10
Town of Trenton					
Initial Transmission		10 of 10	10 of 10	10 of 10	10 of 10
Load Test		7 of 7	4 of 4	8 of 8	5 of 5
Load Test Results		28 of 28	22 of 22	33 of 33	24 of 24

In the second round of testing, WEC staff successfully transmitted election results from each of the three municipalities. The test script calls for the verification of several certification standards and

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 16 of 61

then requires 10 results sets to be transmitted from each tabulator. The machines were able to successfully transmit multiple results with a 100% success rate during this portion of testing. The functional testing concluded with a load test during which WEC staff attempted to transmit results simultaneously from all the machines for a set period of time.

Green County

On April 27, 2021, WEC staff conducted tests on the Democracy Suite 5.5-C and 5.5-CS modem component in three municipalities in Green County: Town of Monroe, City of Monroe, and Village of Browntown. DVS conducted pre-testing of the Democracy Suite 5.5-C and 5.5-CS modem components in Green County prior to WEC testing. An ICE and ICP2, each equipped with Verizon modems, were tested in all three municipalities. The same test script used in Washington County was also used during this portion of the test campaign.

Green County (Analog)					
		ICE		ICP2	
		Standard	Express	Standard	Express
Town of Monroe					
Initial Transmission		10 of 10	5 of 5	10 of 10	5 of 5
Load Test		4 of 5	3 of 3	4 of 6	5 of 5
City of Monroe					
Initial Transmission		10 of 10	5 of 5	10 of 10	5 of 5
Load Test		5 of 5	4 of 4	5 of 7	6 of 7
Village of Browntown					
Initial Transmission		10 of 10	5 of 5	10 of 10	5 of 5
Load Test		5 of 5	3 of 4	5 of 6	1 of 4
Load Test Results		14 of 15	10 of 11	14 of 19	12 of 16

WEC staff successfully transmitted election results from each of the three municipalities. The test script calls for the verification of several certification standards and then requires 10 results sets to be transmitted from each tabulator. The three machines each were able to successfully transmit results with a 100% success rate during this portion of testing. The functional testing concluded with a load test where WEC staff attempted to transmit results simultaneously from all the machines for a set period of time.

As Green County uses analog modems to transmit election results, the load test saw a few instances of transmission failure. This is normal in analog modem testing and was expected, as three tabulators were all attempting to transmit data concurrently to the county office's single analog phone line.

Walworth County

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 17 of 61

On April 28, 2021, WEC staff conducted tests on the Democracy Suite 5.5-C and 5.5-CS modem component in three municipalities in Walworth County: City of Elkhorn, City of Lake Geneva, and Village of Fontana. DVS conducted pre-testing of the Democracy Suite 5.5-C and 5.5-CS modem components in Green County prior to WEC testing. An ICE and ICP2, each equipped with Verizon modems, were tested in all three municipalities. The same test script used in Washington and Green Counties was also used during this portion of the test campaign.

Walworth County (Wireless)					
		ICE		ICP2	
		Standard	Express	Standard	Express
City of Elkhorn					
Initial Transmission		10 of 10	10 of 10	10 of 10	10 of 10
Load Test		11 of 11	11 of 11	10 of 10	14 of 14
City of Lake Geneva					
Initial Transmission		10 of 10	10 of 10	10 of 10	10 of 10
Load Test		9 of 9	10 of 10	11 of 11	11 of 11
Village of Fontana					
Initial Transmission		10 of 10	10 of 10	10 of 10	10 of 10
Load Test		8 of 8	8 of 8	9 of 9	10 of 10
Load Test Results		28 of 28	29 of 29	30 of 30	35 of 35

WEC staff successfully transmitted election results from each of the three municipalities. The test script calls for the verification of several certification standards and then requires 10 results sets to be transmitted from each tabulator. The three machines each were able to successfully transmit results with an 100% success rate during this portion of testing. The functional testing concluded with a load test where WEC staff attempted to transmit results simultaneously from all the machines for a set period of time.

Public Demonstration

A public demonstration of Democracy Suite 5.5-C and 5.5-CS was held on April 22, 2021 from 4:30 p.m. to 5:30 p.m. at the WEC office in Madison and virtually via Zoom. The public meeting is designed to allow members of the public the opportunity to use the voting system and to provide comment. This was the first time a hybrid meeting was held as part of a voting equipment test. Previous public demonstrations were held exclusively in person. As there were zero attendees in person for the public demonstration, representatives from DVS offered a presentation of the components of Democracy Suite 5.5-C and 5.5-CS to the virtual attendees. Following the demonstration of system components, DVS representatives and WEC staff took direct questions from members of the public for the remainder of the meeting.

Wisconsin Elections Commission Voting Equipment Review Panel Meeting

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 18 of 61

In an effort to continue to solicit valuable feedback from local election officials and community advocates during the voting equipment approval process, the Wisconsin Elections Commission formed a Voting Equipment Review Panel. The Voting Equipment Review Panel is composed of municipal and county clerks, representatives of the disability community, and advocates for the interests of the voting public. Wis. Admin. Code EL §7.02(2), permits the agency to use a panel of local election officials and electors to assist in the review of voting systems. Like the public demonstration, this meeting has historically been held only in person. The Voting Equipment Review Panel meeting for the current test campaign was, instead, held in a hybrid manner with both in person attendees, as well as those viewing virtually via Zoom. The meeting was also broadcast for viewing by public attendees. However, direct participation was reserved for Review Panel members.

Four invited participants attended the Voting Equipment Review Panel Meeting in person, while a further three attended virtually. The meeting took place at the WEC office in Madison on April 22, 2021 from 2:00 p.m. to 3:30 p.m. DVS provided a demonstration of Democracy Suite 5.5-C and 5.5-CS with attendees encouraged to test the equipment. The modeming component of Democracy Suite 5.5-C and 5.5-CS was discussed but not demonstrated during the meeting. Comments and feedback from the Voting Equipment Review Panel meeting are included in Appendix G.

Statutory Compliance

Wis. Stat. § 5.91 provides the following requirements voting systems must meet to be approved for use in Wisconsin. Please see the text below of each requirement and staff's analysis of the Democracy Suite 5.5-C and 5.5-CS compliance with the standards.

§ 5.91 (1)
The voting system enables an elector to vote in secret.
Staff Analysis
The DVS voting systems meet this requirement by allowing a voter to vote a paper ballot in the privacy of a voting booth or at the accessible voting station without assistance.

§ 5.91 (3)
The voting system enables the elector, for all elections, except primary elections, to vote for a ticket selected in part from the nominees of one party, and in part from nominees from other parties and write-in candidates
Staff Analysis
The DVS voting systems allow voter to split their ballot among as many parties as they wish during any election that is not a partisan primary.

§ 5.91 (4)

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 19 of 61

The voting system enables an elector to vote for a ticket of his or her own selection for any person for any office for whom he or she may desire to vote whenever write-in votes are permitted.
Staff Analysis
The DVS voting systems allow write-ins where permitted.

§ 5.91 (5)
The voting systems accommodate all referenda to be submitted to electors in the form provided by law.
Staff Analysis
The DVS voting systems meet this requirement. Referenda included as part of testing were accurately tabulated by all Democracy Suite 5.5-C and 5.5-CS components.

§ 5.91 (6)
The voting system permits an elector in a primary election to vote for the candidates of the recognized political party of his or her choice, and the system rejects any ballot on which votes are cast in the primary of more than one recognized political party, except where a party designation is made or where an elector casts write-in votes for candidates of more than one party on a ballot that is distributed to the elector.
Staff Analysis
The DVS voting systems can be configured to always reject crossover votes without providing an opportunity for the voter to override. The system can also be programmed to provide a warning screen to the voter that identifies any crossover voted contest. Either one of these programming options allows these systems to meet this requirement. The warning screen provides options where the voter can choose to have their ballot returned to them or they can cast the ballot without correcting the crossover vote. The use of the override function was previously prohibited by statute, but Wis. Stats. §5.85(2)(b) expressly allows for the optional use of the override function in event of an overvote and the WEC has applied the same standard to the use of the override function in the event of crossover vote.

§ 5.91 (7)
The voting system enables the elector to vote at an election for all persons and offices for whom and for which the elector is lawfully entitled to vote; to vote for as many persons for an office as the elector is entitled to vote for; to vote for or against any question upon which the elector is entitled to vote; and it rejects all choices recorded on a ballot for an office or a measure if the number of choices exceeds the number which an elector is entitled to vote for on such

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 20 of 61

office or on such measure, except where an elector casts excess write-in votes upon a ballot that is distributed to the elector.
Staff Analysis
The DVS voting systems can be configured to always reject overvotes without providing an opportunity for the voter to override. The system can also be programmed to provide a warning screen to the voter that identifies any overvoted contest. Either one of these programming options allows these systems to meet this requirement. The warning screen provides options where the voter can choose to have their ballot returned to them or they can cast the ballot without correcting the overvote. The use of the override function was previously prohibited by statute, but Wis. Stats. §5.85(2)(b) expressly allows for the optional use of the override function in event of an overvote.

§ 5.91 (8)
The voting system permits an elector at a General Election by one action to vote for the candidates of a party for President and Vice President or for Governor and Lieutenant Governor.
Staff Analysis
The DVS voting systems meet this requirement. Traditional paper ballots utilized by the ICE and ICP2, as well as the ICX DRE and ICX BMD candidate screens, present the two candidates in these contests as a single choice.

§ 5.91 (9)
The voting system prevents an elector from voting for the same person more than once, except for excess write-in votes upon a ballot that is distributed to the elector.
Staff Analysis
The DVS voting systems meet this requirement.

§ 5.91 (10)
The voting system is suitably designed for the purpose used, of durable construction, and is usable safely, securely, efficiently, and accurately in the conduct of elections and counting of ballots.
Staff Analysis
The DVS voting systems meet this requirement.

§ 5.91 (11)
The voting system records and counts accurately every vote and maintains a cumulative tally of the total votes cast that is retrievable in the event of a

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 21 of 61

power outage, evacuation or malfunction so that the records of votes cast prior to the time that the problem occurs is preserved.
Staff Analysis
The DVS voting systems meet this requirement. Tabulation equipment components of Democracy Suite 5.5-C and 5.5-CS image every ballot cast and saves to a detachable memory device for retrieval if necessary.

§ 5.91 (12)
The voting system minimizes the possibility of disenfranchisement of electors as the result of failure to understand the method of operation or utilization or malfunction of the ballot, voting system, or other related equipment or materials.
Staff Analysis
The DVS voting systems can be programmed to provide warning screens to the voter that identifies any problem with their ballot. The warning screens provide an explanation of the problem and allow the voter to have their ballot returned to them to review and correct the error. The systems can be configured to always reject overvotes and crossover votes without providing an opportunity for the voter to override.

§ 5.91 (13)
The automatic tabulating equipment authorized for use in connection with the system includes a mechanism which makes the operator aware of whether the equipment is malfunctioning in such a way that an inaccurate tabulation of the votes could be obtained.
Staff Analysis
The DVS voting systems meet this requirement. In the event of attempted unauthorized access, the tabulation equipment locks down and provides a port protect warning to election inspectors describing any issues perceived by the machine

§ 5.91 (14)
The voting system does not use any mechanism by which a ballot is punched or punctured to record the votes cast by an elector.
Staff Analysis
The DVS system does not use any such mechanism to record votes.

§ 5.91 (15)
The voting system permits an elector to privately verify the votes selected by the elector before casting his or her ballot.
Staff Analysis

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 22 of 61

The DVS voting systems meet this requirement through the use of hand-marked paper ballots and accessible voting equipment that provides both an electronic ballot review screen and a marked paper ballot that can be reviewed before tabulation.

§ 5.91 (16)
The voting system provides an elector the opportunity to change his or her votes and to correct any error or to obtain a replacement for a spoiled ballot prior to casting his or her ballot.
Staff Analysis
The DVS voting systems meet this requirement. Traditional paper ballots can be changed and/or spoiled at any point up to being placed in the tabulator. ICE BMD and ICE DRE ballots are printed for the voter to review prior to casting and can be spoiled or rejected and revoted at will by the voter.

§ 5.91 (17)
Unless the ballot is counted at a central counting location, the voting system includes a mechanism for notifying an elector who attempts to cast an excess number of votes for a single office the ballot will not be counted, and provides the elector with an opportunity to correct his or her ballot or to receive a replacement ballot.
Staff Analysis
The DVS voting systems provides warning screens to the voter that identifies any problem with the ballot. The warning screens provide an explanation of the problem and allow the voter to have their ballot returned to them to review and correct the error. The systems can be configured to always reject overvotes and crossover votes without providing an opportunity for the voter to override.

§ 5.91 (18)
If the voting system consists of an electronic voting machine, the voting system generates a complete, permanent paper record showing all votes cast by the elector, that is verifiable by the elector, by either visual or nonvisual means as appropriate, before the elector leaves the voting area, and that enables a manual count or recount of each vote cast by the elector.
Staff Analysis
Since the DVS voting systems presented for approval require paper ballots to be used to cast votes, and the DRE and BMD equipment automatically provide a physical review of ballots, this requirement is satisfied.

The Help America Vote Act of 2002 (HAVA) also provides the following applicable requirements that voting systems must meet:

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 23 of 61

HAVA § 301(a)(1)(A)
The voting system shall: (i) permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted; (ii) provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error); and (iii) if the voter selects votes for more than one candidate for a single office – (I) notify the voter that the voter has selected more than one candidate for a single office on the ballot; (II) notify the voter before the ballot is cast and counted of the effect of casting multiple votes for the office; and, (III) provide the voter with the opportunity to correct the ballot before the ballot is cast and counted
HAVA § 301(a)(1)(C)
The voting system shall ensure that any notification required under this paragraph preserves the privacy of the voter and the confidentiality of the ballot.
HAVA § 301(a)(3)(A)
The voting system shall— (A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as other voters
Staff Analysis
The Democracy Suite 5.5-C and 5.5-CS voting system components meet these requirements through the inclusion of options for ADA-compliant voting machines which municipalities can choose to employ.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 24 of 61

Recommendations

Staff has reviewed the application materials, including the technical data package and testing lab report, and examined the results from the functional and modeming test campaigns to determine if these systems are compliant with both state and federal certification laws. Democracy Suite 5.5-C and 5.5-CS complies with all applicable state and federal requirements. The voting system components met all standards over three mock elections and staff determined they can successfully run a transparent, fair, and secure election in compliance with Wisconsin Statutes. The system also helps grant access to the electoral process for individuals with disabilities with the inclusion of the ICE tabulator BMD, ICX BMD, and ICX DRE voting devices.

1. WEC staff recommends approval of DVS voting system Democracy Suite 5.5-C and 5.5-CS and components set forth in Appendix A of this report, as described below in item 3. This voting system accurately completed the three mock elections and was able to accommodate the voting requirements of the Wisconsin election process. This recommendation is based on the EAC certification, VSTL report provided by Pro V&V and on this voting system successfully completing Wisconsin functional testing as dictated by the *Voting Systems Standards, Testing Protocols and Procedures Pertaining to the Use of Communication Devices in Wisconsin*.
2. WEC staff recommends that as a continuing condition of the WEC's approval, DVS may not impose customer deadlines contrary to requirements provided in Wisconsin Statutes, as determined by the WEC. In order to enforce this provision, local jurisdictions purchasing DVS equipment shall also include such a provision in their respective purchase contract or amend their contract if such a provision does not currently exist.
3. WEC staff recommends that as a continuing condition of the WEC's approval, that voting systems purchased and installed as part of Democracy Suite 5.5-C and 5.5-CS be configured in the same manner in which they were tested, subject to verification by the Commission or its designee. Once installed, the configuration must remain the same and may not be altered by DVS nor by state, county, or municipal officials except as approved by the Commission.
4. WEC staff recommends that ballots marked with ICE tabulator BMD, ICX BMD, and ICX DRE equipment be included as part of the pre-election public test. ICX BMD ballots will not scan on the tabulation equipment and would have to be hand counted. However, staff recommends the inclusion of these ballots to confirm the programming on the BMD equipment.
5. WEC staff recommends that ICX BMD be certified for hand counting only.
6. WEC staff recommends clerks and election inspectors ensure that external modems are secured prior to, during, and after every election, with proper chain of custody documentation utilized.
7. WEC staff recommends that election inspectors continue to check both the write-in bin and main ballot bin for validly cast write-in votes after the close of polls in each election, and not rely upon the optional write-in report.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 25 of 61

8. WEC staff recommends that any absentee ballot returned by the tabulation equipment with an overvote or crossover vote notification must be reviewed by election inspectors prior to being overridden or remade. If necessary, ballots must be remade pursuant to approved procedures listed in the Election Day and Election Administration manuals.
9. WEC staff recommends that any absentee ballot returned that has been marked with red ink be remade by election inspectors prior to any attempt at processing on the tabulation equipment.
10. WEC staff recommends that as a continuing condition of the WEC's approval, that this system must always be configured to include the following options:
 - a. Automatic rejection of crossover and overvoted ballots with or without the option to override.
 - b. Automatic rejection of all improper ballots except blank ballots.
 - c. Digital ballot images to be captured for all ballots tabulated by the system.
 - d. The ambiguous mark threshold be set to 12%-35%, the same level at which it was tested.
 - e. Automatically return marked ballots to the voter for physical review prior to casting when marked using the ICE tabulator BMD function.
 - f. ICX DRE voting devices must always be programmed allow for physical review and voter confirmation of ballot prior to casting.
 - g. Provide visual warning message, utilizing Commission approved language, to voters when overvotes and crossover votes are detected.
 - h. Voter ballot activation cards used as part of the ICX BMD or DRE be reprogrammed after each use and set to expire after one hour.
 - i. ICX BMD and DRE be programmed to present only one contest per page.
11. As part of this WEC certification, only equipment included in this certificate can be used together to conduct an election in Wisconsin. Previous system versions that were approved for use by the WEC, former Elections Board, or the former G.A.B. are not compatible with Democracy Suite 5.5-C and 5.5-CS and are not to be used in conjunction with the equipment components of Democracy Suite 5.5-C and 5.5-CS as submitted for approval. If a jurisdiction upgrades to Democracy Suite 5.5-C and 5.5-CS, it needs to upgrade each and every component of the voting system to the requirements of what is approved herein.
12. WEC staff recommends that as a condition of approval, DVS shall abide by applicable Wisconsin public records laws. If, pursuant to a proper public records request, the customer receives a request for matters that might be proprietary or confidential, customer will notify DVS, providing the same with the opportunity to either provide customer with the record that is requested for release to the requestor, or shall advise customer that DVS objects to the release of the information, and provide the legal and factual basis of the objection. If for any reason, the customer concludes that customer is obligated to provide such records, DVS shall provide such records immediately upon customer's request. DVS shall negotiate and specify retention and public records production costs in writing with customers prior to charging said fees. In absence of meeting such conditions of approval, DVS shall not charge customer for work performed pursuant to a proper public records request, except for the "actual, necessary, and direct" charge of responding to the records request, as that is defined and interpreted in Wisconsin law, plus shipping, handling, and chain of custody.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 26 of 61

13. The Wisconsin application for approval contains a condition that requires the vendor to reimburse the WEC for all costs associated with the testing campaign and certification process. DVS agreed to this requirement on the applications submitted to WEC on September 3, 2020 requesting the approval of Democracy Suite 5.5-C and 5.5-CS.

A. Proposed Motion

MOTION: The Wisconsin Elections Commission adopts the staff's recommendations for approval of the DVS voting system's Application for Approval of Democracy Suite 5.5-C and 5.5-CS, including the conditions described above.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 27 of 61

Appendices

- Appendix A: Hardware and Software Components
- Appendix B: Screen Shots of Approved Tabulator Language for Voter Notification Screens
- Appendix C: Wisconsin Statutes § 5.91
- Appendix D: Wisconsin Administrative Code Ch. EL 7
- Appendix E: Election Assistance Commission Certification and Scope Report
- Appendix F: Voting Systems Standards, Testing Protocols and Procedures Pertaining to the Use of Communication Devices in Wisconsin
- Appendix G: Wisconsin Voting Equipment Review Panel Feedback

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 28 of 61

Appendix A: Hardware and Software Components

Equipment	Hardware Versions(s)	Firmware Version	Type
ImageCast X with BMD	Avalue SID-15V-Z37 Avalue SID-21V-Z37 Avalue HID-21V-BTX	5.5.15.2	Accessible touchscreen ballot marking device
ImageCast X DRE with VVPT	Avalue HID-21V-BTX	5.5.15.2	Accesible touchscreen direct recording electronic device
ImageCast X DRE with Report Printer	Avalue HID-21V-BTX	5.5.15.2	Accesible touchscreen direct recording electronic device
ImageCast Evolution	PCOS-410A	5.5.6.5	Polling place optical scan tabulator
ImageCast Evolution (Dual Monitor)	PCOS-410A AOC e1649FWU	5.5.6.5	Polling place optical scan tabulator
ImageCast Precinct	PCOS-320A PCOS-320C PCOS-321C	5.5.41.3	Polling place optical scan tabulator
ImageCast Precinct (ICP2)	PCOS-330A	5.5.2.1	Polling place optical scan tabulator
ImageCast Central	Canon DR-G2140 Canon DR-G1130 Canon DR-M160-II Canon DR-M260 InoTec HiPro 821	5.5.41.0002	High-speed central count scanner

Software Component	Version
Election Management System (EMS)	5.5.40.2
ImageCast Voter Activation	5.5.40.2
Results Transfer Manager (RTM)	5.5.40.2

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 29 of 61

Appendix B: Screen Shots of Approved Language for Tabulator Voter Notification Screens

- ICE Partisan Selection Screen/Confirmation Screen (Accessible Voting Mode)

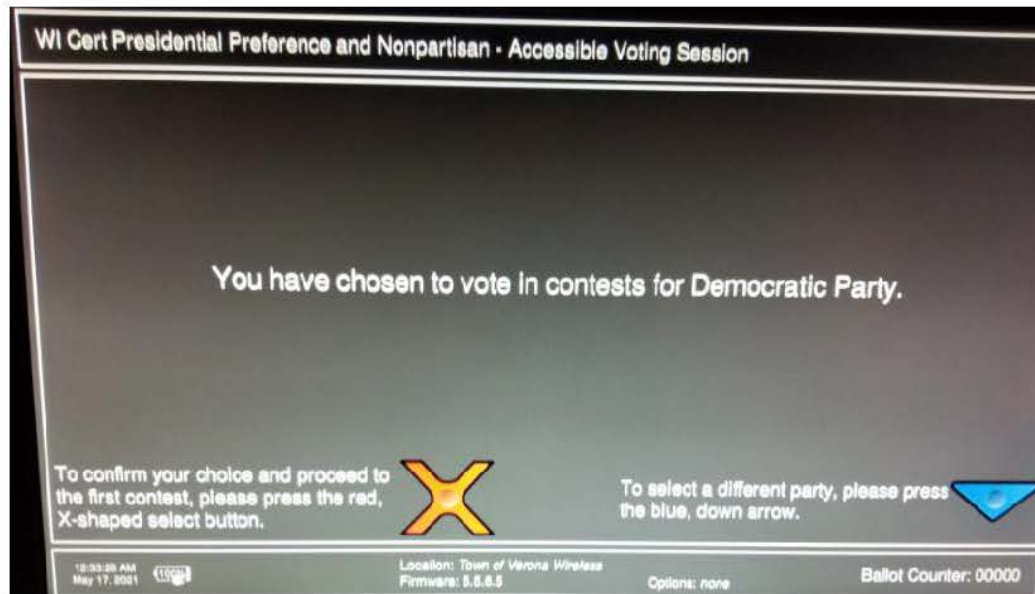


Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 30 of 61

- **ICE Crossover Vote Notification Screen**

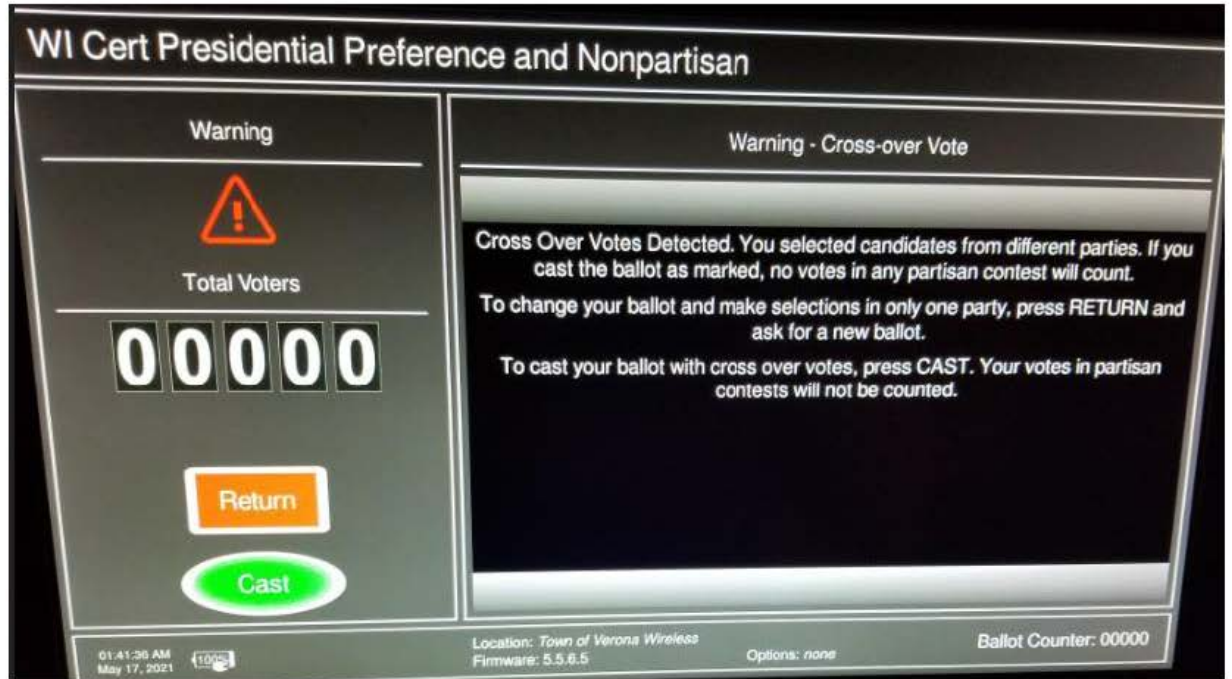


Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 31 of 61

- **ICE Overvote Notification Screen**

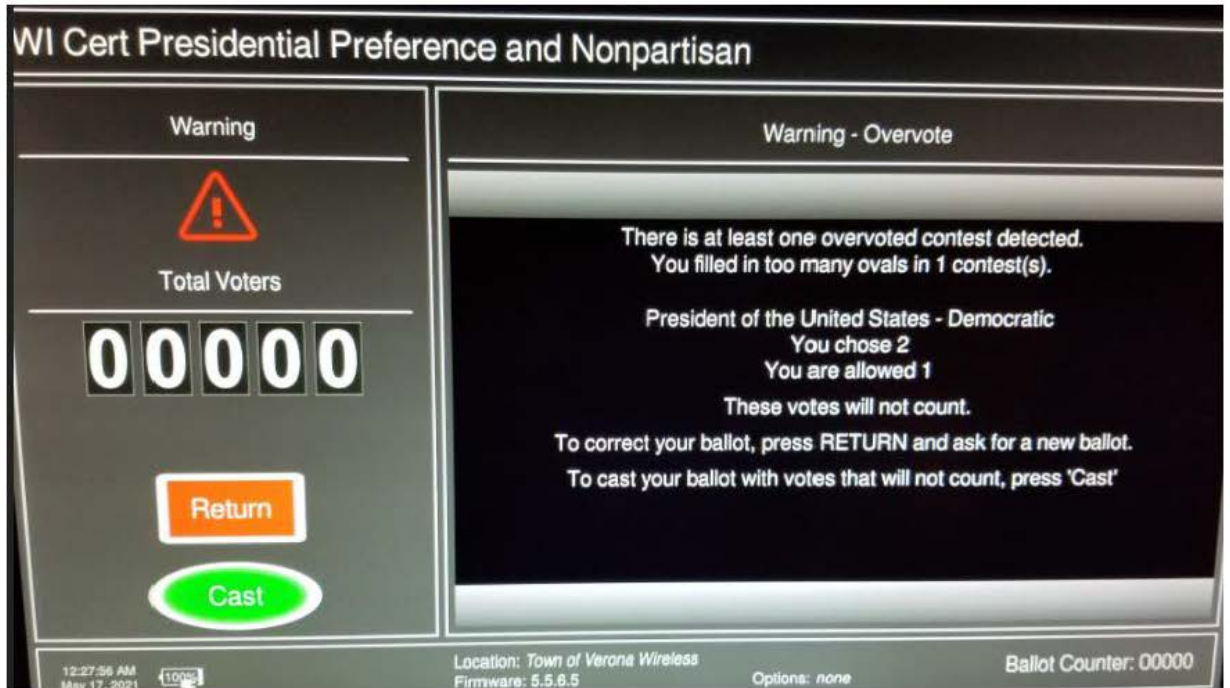


Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 32 of 61

- ICP2 Crossover Vote Screens

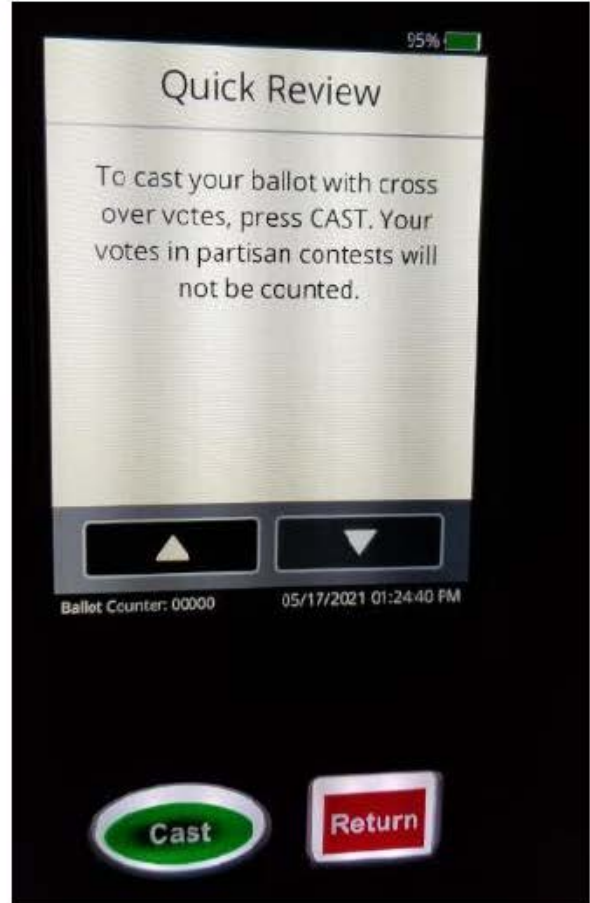
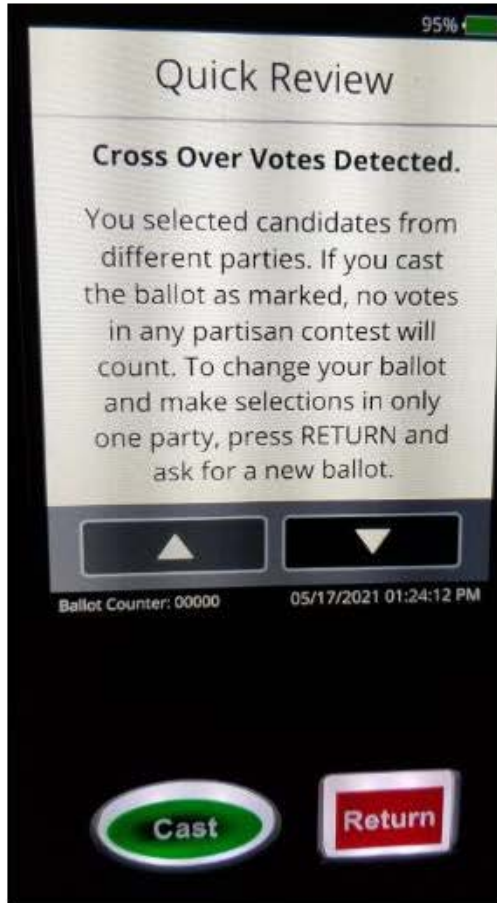


Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 33 of 61

- ICP2 Overvote Screens

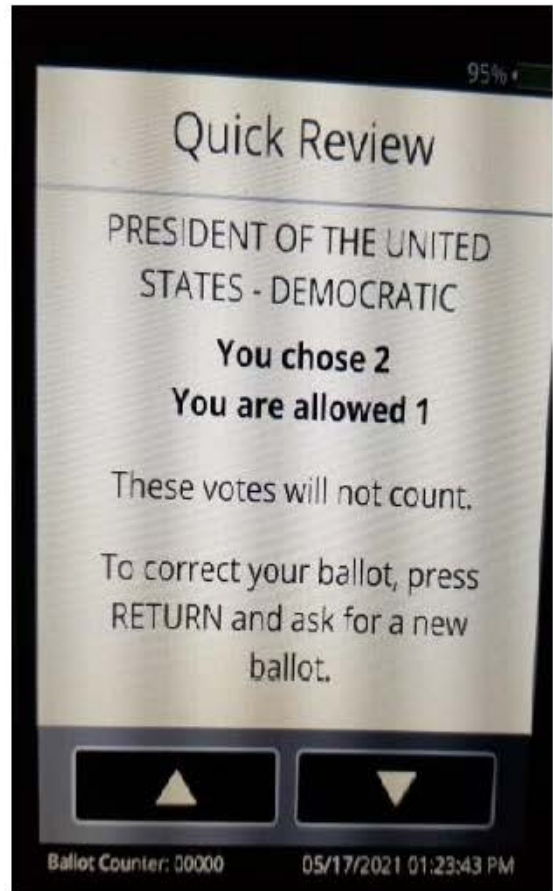


Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 34 of 61

- **ICX Partisan Primary Selection Screen**
 - **Prompt reads "In the Partisan Primary: You may vote in only ONE party. Once you choose a party, you will only see contests and candidates for that party's primary. Please select your party preference."**

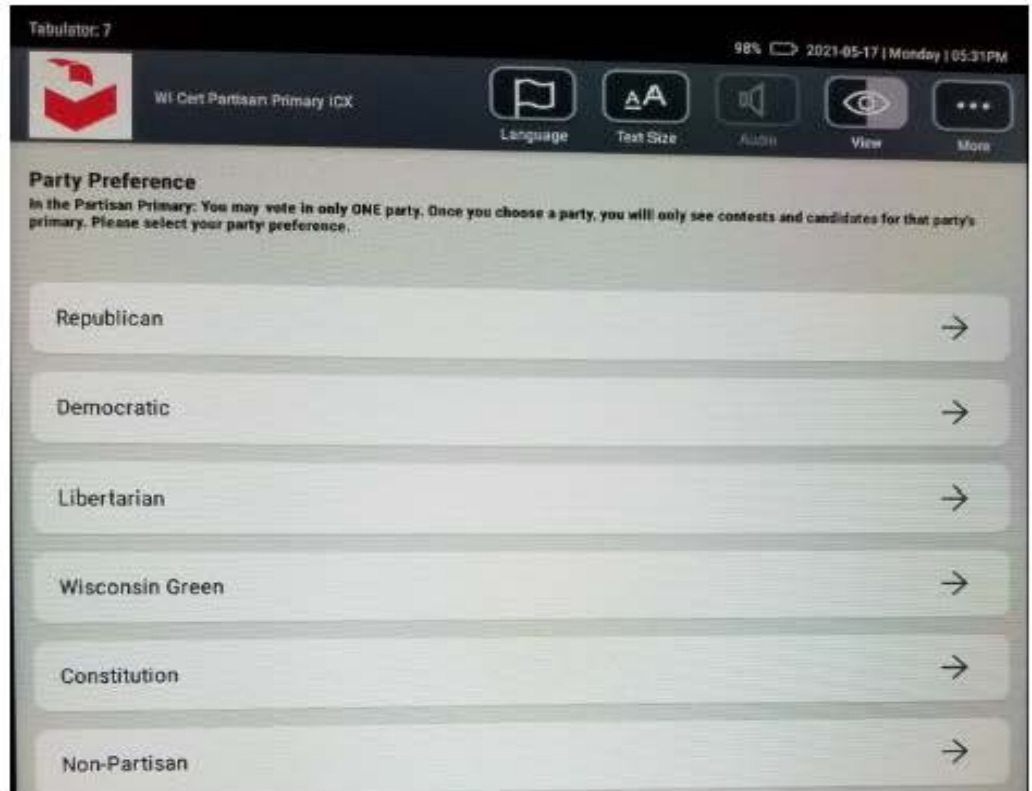


Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 35 of 61

- **ICX Presidential Preference Primary Language**

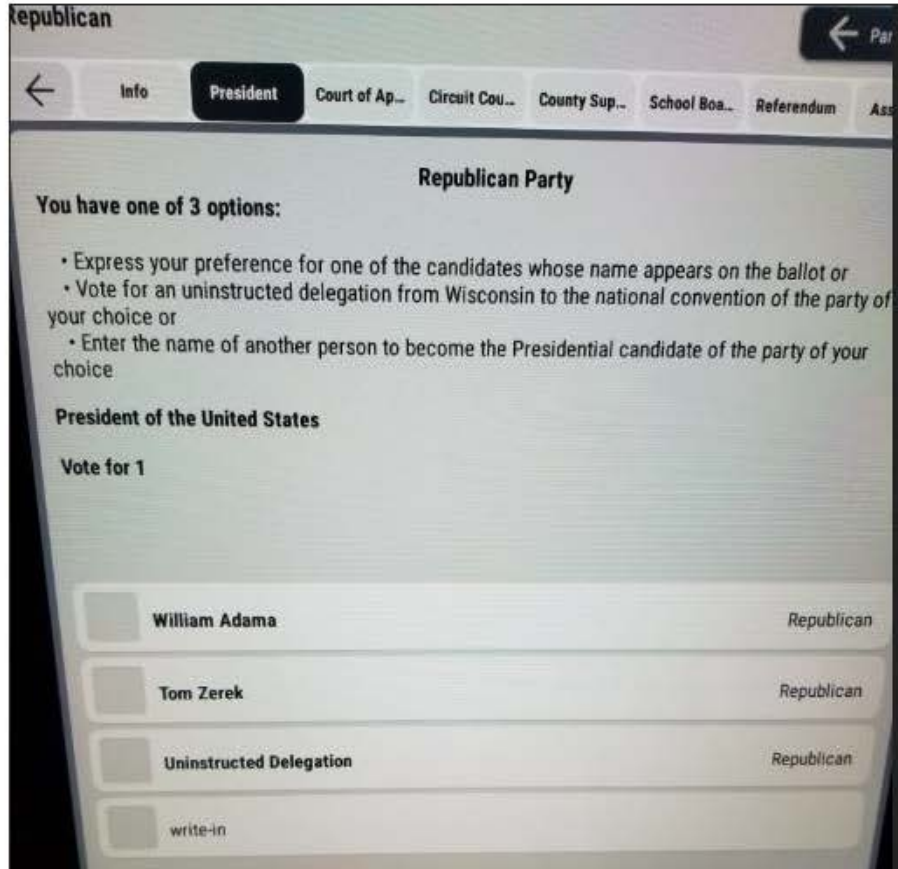


Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 36 of 61

Appendix C: Wis. Stat. § 5.91

5.91 Requisites for approval of ballots, devices and equipment. No ballot, voting device, automatic tabulating equipment, or related equipment and materials to be used in an electronic voting system may be utilized in this state unless it is certified by the commission. The commission may revoke its certification of any ballot, device, equipment, or materials at any time for cause. The commission may certify any such voting device, automatic tabulating equipment, or related equipment or materials regardless of whether any such item is approved by the federal election assistance commission, but the commission may not certify any ballot, device, equipment, or material to be used in an electronic voting system unless it fulfills the following requirements:

- (1) It enables an elector to vote in secrecy and to select the party for which an elector will vote in secrecy at a partisan primary election.
- (3) Except in primary elections, it enables an elector to vote for a ticket selected in part from the nominees of one party, and in part from the nominees of other parties, and in part from independent candidates and in part of candidates whose names are written in by the elector.
- (4) It enables an elector to vote for a ticket of his or her own selection for any person for any office for whom he or she may desire to vote whenever write-in votes are permitted.
- (5) It accommodates all referenda to be submitted to the electors in the form provided by law.
- (6) The voting device or machine permits an elector in a primary election to vote for the candidates of the recognized political party of his or her choice, and the automatic tabulating equipment or machine rejects any ballot on which votes are cast in the primary of more than one recognized political party, except where a party designation is made or where an elector casts write-in votes for candidates of more than one party on a ballot that is distributed to the elector.
- (7) It permits an elector to vote at an election for all persons and offices for whom and for which the elector is lawfully entitled to vote; to vote for as many persons for an office as the elector is entitled to vote for; to vote for or against any question upon which the elector is entitled to vote; and it rejects all choices recorded on a ballot for an office or a measure if the number of choices exceeds the number which an elector is entitled to vote for on such office or on such measure, except where an elector casts excess write-in votes upon a ballot that is distributed to the elector.
- (8) It permits an elector, at a presidential or gubernatorial election, by one action to vote for the candidates of a party for president and vice president or for governor and lieutenant governor, respectively.
- (9) It prevents an elector from voting for the same person more than once for the same office, except where an elector casts excess write-in votes upon a ballot that is distributed to the elector.
- (10) It is suitably designed for the purpose used, of durable construction, and is usable safely, securely, efficiently and accurately in the conduct of elections and counting of ballots.
- (11) It records correctly and counts accurately every vote properly cast and maintains a cumulative tally of the total votes cast that is retrievable in the event of a power outage, evacuation or malfunction so that the records of votes cast prior to the time that the problem occurs is preserved.
- (12) It minimizes the possibility of disenfranchisement of electors as the result of failure to understand the method of operation or utilization or malfunction of the ballot, voting device, automatic tabulating equipment or related equipment or materials.
- (13) The automatic tabulating equipment authorized for use in connection with the system includes a mechanism which makes the operator aware of whether the equipment is malfunctioning in such a way that an inaccurate tabulation of the votes could be obtained.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 37 of 61

- (14) It does not employ any mechanism by which a ballot is punched or punctured to record the votes cast by an elector.
- (15) It permits an elector to privately verify the votes selected by the elector before casting his or her ballot.
- (16) It provides an elector with the opportunity to change his or her votes and to correct any error or to obtain a replacement for a spoiled ballot prior to casting his or her ballot.
- (17) Unless the ballot is counted at a central counting location, it includes a mechanism for notifying an elector who attempts to cast an excess number of votes for a single office that his or her votes for that office will not be counted, and provides the elector with an opportunity to correct his or her ballot or to receive and cast a replacement ballot.
- (18) If the device consists of an electronic voting machine, it generates a complete, permanent paper record showing all votes cast by each elector, that is verifiable by the elector, by either visual or nonvisual means as appropriate, before the elector leaves the voting area, and that enables a manual count or recount of each vote cast by the elector.

History: 1979 c. 311; 1983 a. 484; 1985 a. 304; 2001 a. 16; 2003 a. 265; 2005 a. 92; 2011 a. 23, 32; 2015 a. 118 s. 266 (10); 2015 a. 261; 2017 a. 365 s. 111.

Cross-reference: See also ch. EL 7, Wis. adm. code.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 38 of 61

Appendix D: Wis. Admin. Code Ch. EL 7

Chapter EL 7

APPROVAL OF ELECTRONIC VOTING EQUIPMENT

EL 7.01 Application for approval of electronic voting system.

EL 7.02 Agency testing of electronic voting system.

EL 7.03 Continuing approval of electronic voting system.

Note: Chapter ElBd 7 was renumbered chapter GAB 7 under s. 13.92 (4) (b) 1., Stats., and corrections made under s. 13.92 (4) (b) 7., Stats., [Register April 2008 No. 628](#). **Chapter GAB 7 was renumbered Chapter EL 7 under s. 13.92 (4) (b) 1., Stats., Register June 2016 No. 726.**

EL 7.01 Application for approval of electronic voting system.

(1) An application for approval of an electronic voting system shall be accompanied by all of the following:

(a) A signed agreement that the vendor shall pay all costs, related to approval of the system, incurred by the elections commission, its designees and the vendor.

(b) Complete specifications for all hardware, firmware and software.

(c) All technical manuals and documentation related to the system.

(d) Complete instruction materials necessary for the operation of the equipment and a description of training available to users and purchasers.

(e) Reports from an independent testing authority accredited by the national association of state election directors (NASSED) demonstrating that the voting system conforms to all the standards recommended by the federal elections commission.

(f) A signed agreement requiring that the vendor shall immediately notify the elections commission of any modification to the voting system and requiring that the vendor will not offer, for use, sale or lease, any modified voting system, if the elections commission notifies the vendor that the modifications require that the system be approved again.

(g) A list showing all the states and municipalities in which the system has been approved for use and the length of time that the equipment has been in use in those jurisdictions.

(2) The commission shall determine if the application is complete and, if it is, shall so notify the vendor in writing. If it is not complete, the elections commission shall so notify the vendor and shall detail any insufficiencies.

(3) If the application is complete, the vendor shall prepare the voting system for three mock elections, using offices, referenda

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 39 of 61

questions and candidates provided by the elections commission.

History: Cr. Register, June, 2000, No. 534, eff. 7-1-00; correction in (1) (a), (f), (2), (3) made under s. 13.92 (4) (b) 6., Stats., Register June 2016 No. 726.

EL 7.02 Agency testing of electronic voting system.

(1) The elections commission shall conduct a test of a voting system, submitted for approval under s. EL 7.01, to ensure that it meets the criteria set out in s. 5.91, Stats. The test shall be conducted using a mock election for the partisan primary, a mock general election with both a presidential and gubernatorial vote, and a mock nonpartisan election combined with a presidential preference vote.

(2) The elections commission may use a panel of local election officials and electors to assist in its review of the voting system.

(3) The elections commission may require that the voting system be used in an actual election as a condition of approval.

History: Cr. Register, June, 2000, No. 534, eff. 7-1-00; correction in (1) to (3) made under s. 13.92 (4) (b) 6., Stats., and correction in (1) made under s. 13.92 (4) (b) 7., Stats., Register June 2016 No. 726.

EL 7.03 Continuing approval of electronic voting system.

(1) The elections commission may revoke the approval of any existing electronic voting system if it does not comply with the provisions of this chapter. As a condition of maintaining the elections commission's approval for the use of the voting system, the vendor shall inform the elections commission of all changes in the hardware, firmware and software and all jurisdictions using the voting system.

(2) The vendor shall, at its own expense, furnish, to an agent approved by the elections commission, for placement in escrow, a copy of the programs, documentation and source code used for any election in the state.

(3) The electronic voting system must be capable of transferring the data contained in the system to an electronic recording medium, pursuant to the provisions of s. 7.23, Stats.

(4) The vendor shall ensure that election results can be exported on election night into a statewide database developed by the elections commission.

(5) For good cause shown, the elections commission may exempt any electronic voting system from strict compliance with this chapter.

History: Cr. Register, June, 2000, No. 534, eff. 7-1-00; correction in (1), (4), (5)

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 40 of 61

made under s. 13.92 (4) (b) 6., Stats. and corrections in (5) made under s. 13.92 (4) (b) 7., Stats., and s. 35.17, Stats., Register June 2016 No. 726.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 41 of 61

Appendix E: EAC Certification and Scope Report

	United States Election Assistance Commission	
Certificate of Conformance		
Dominion Voting Systems Democracy Suite 5.5-C		
<p>The voting system identified on this certificate has been evaluated at an accredited voting system testing laboratory for conformance to the <i>Voluntary Voting System Guidelines Version 1.0 (VVSG 1.0)</i>. Components evaluated for this certification are detailed in the attached Scope of Certification document. This certificate applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been verified by the EAC in accordance with the provisions of the <i>EAC Voting System Testing and Certification Program Manual</i> and the conclusions of the testing laboratory in the test report are consistent with the evidence adduced. This certificate is not an endorsement of the product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.</p>		
Product Name:	<u>Democracy Suite</u>	
Model or Version:	<u>5.5-C</u>	
Name of VSTL:	<u>Pro V&V</u>	 _____ <i>Executive Director</i>
EAC Certification Number:	<u>DVS-DemSuite5.5-C</u>	
Date Issued:	<u>July 9, 2020</u>	Scope of Certification Attached

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 42 of 61

Manufacturer: *Dominion Voting Systems (DVS)*
System Name: *Democracy Suite 5.5-C*
Certificate: *DVS-DemSuite5.5-C*

Laboratory: *Pro V&V*
Standard: *VVSG 1.0 (2005)*
Date: *07/02/2020*



Scope of Certification

This document describes the scope of the validation and certification of the system defined above. Any use, configuration changes, revision changes, additions or subtractions from the described system are not included in this evaluation.

Significance of EAC Certification

An EAC certification is an official recognition that a voting system (in a specific configuration or configurations) has been tested to and has met an identified set of Federal voting system standards. An EAC certification is not:

- An endorsement of a Manufacturer, voting system, or any of the system's components.
- A Federal warranty of the voting system or any of its components.
- A determination that a voting system, when fielded, will be operated in a manner that meets all HAVA requirements.
- A substitute for State or local certification and testing.
- A determination that the system is ready for use in an election.
- A determination that any particular component of a certified system is itself certified for use outside the certified configuration.

Representation of EAC Certification

Manufacturers may not represent or imply that a voting system is certified unless it has received a Certificate of Conformance for that system. Statements regarding EAC certification in brochures, on Web sites, on displays, and in advertising/sales literature must be made solely in reference to specific systems. Any action by a Manufacturer to suggest EAC endorsement of its product or organization is strictly prohibited and may result in a Manufacturer's suspension or other action pursuant to Federal civil and criminal law.

System Overview:

The D-Suite 5.5-C Voting System is a paper-based optical scan voting system with a hybrid paper/DRE option consisting of the following major components: The Election Management System (EMS), the ImageCast Central (ICC), the ImageCast Precinct (ICP and ICP2), the ImageCast Evolution (ICE), the ImageCast X (ICX) DRE w/ Reports Printer, ImageCast X (ICX) DRE w/ voter-verifiable paper audit trail (VVPAT), and the ImageCast X ballot marking device (BMD). The D-Suite 5.5-C Voting System configuration is a modification from the EAC approved D-Suite 5.5-B system configuration.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 43 of 61

Language capability:

This section provides information describing the languages supported by the various components of the system.

Language	ICE	ICP	ICP2	ICX
Alaska Native	Yes, if using Latin alphabet	Yes	No	No
Apache	Audio only	Audio only	No	No
Bengali	Yes	Yes	Yes	Yes
Chinese	Yes	Yes	Yes	Yes
English	Yes	Yes	Yes	Yes
Eskimo	Yes, if using Latin alphabet	Yes	No	No
Filipino	Yes, if using Latin alphabet	Yes	Yes	No
French	Yes	Yes	No	Yes
Hindi	Yes	Audio only	Yes	Yes
Japanese	Yes	Yes	Yes	Yes
Jicarilla	Audio only	Audio only	No	No
Keres	Audio only	Audio only	No	No
Khmer	Yes	Audio only	No	No
Korean	Yes	Yes	Yes	Yes
Navajo	Audio only	Audio only	No	No
Seminole	Audio only	Audio only	No	No
Spanish	Yes	Yes	Yes	Yes
Tagalog	No	No	No	Yes
Thai	Yes	Audio only	Yes	Yes
Towa	Audio only	Audio only	No	No
Ute	Audio only	Audio only	No	No
Vietnamese	Yes	Yes	Yes	Yes
Yuman	Audio only	Audio only	No	No

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 45 of 61

Components Included:

This section provides information describing the components and revision level of the primary components included in this Certification.

Voting System Software Components:

System Component	Software or Firmware Version	Operating System or COTS	Comments
EMS Election Event Designer (EED)	5.5.40.2	Windows 10 Pro	EMS
EMS Results Tally and Reporting (RTR)	5.5.40.2	Windows 10 Pro	EMS
EMS Application Server	5.5.40.2	Windows Server 2012 R2 Windows 10 Pro	EMS
EMS File System Service (FSS)	5.5.40.2	Window 10 Pro	EMS
EMS Audio Studio (AS)	5.5.40.2	Windows 10 Pro	EMS
EMS Data Center Manager (DCM)	5.5.40.2	Windows Server 2012 R2 Windows 10 Pro	EMS
EMS Election Data Translator (EDT)	5.5.40.2	Windows 10 Pro	EMS
ImageCast Voter Activation (ICVA)	5.5.40.2	Windows 10 Pro	EMS
EMS Adjudication (ADJ)	5.5.40.1	Windows 10 Pro	EMS
EMS Adjudication Services	5.5.40.1	Windows 10 Pro	EMS
Smart Card Helper Service (SCHS)	5.5.40.2	Windows 10 Pro	EMS
Election Firmware	5.5.41.3	uClinux	ICP
Firmware Updater	5.5.41.3	uClinux	ICP
Firmware Extractor	5.5.41.3	uClinux	ICP
Kernel (uClinux)	5.5.41.3	Modified COTS	ICP
Boot Loader (COLILO)	20040221	Modified COTS	ICP
Asymmetric Key Generator	5.5.41.3	uClinux	ICP
Asymmetric Key Exchange Utility	5.5.41.3	uClinux	ICP
Firmware Extractor (Technician Key)	5.5.41.3	uClinux	ICP
ICP2 Application	5.5.2.1	uClinux	ICP2
ICP2 Update Card	5.5.2.1	uClinux	ICP2
Voting Machine	5.5.6.5	Ubuntu Linux	ICE
Election Application	5.5.6.5	Ubuntu Linux	ICE
ImageCast Central Application	5.5.41.0002	Windows 10 Pro	ICC
ICX Application	5.5.15.2	Android 5.1.1 (ICX Prime) Android 4.4.4 (ICX Classic)	ICX

Voting System Platform:

System Component	Version	Operating System or COTS	Comments
Microsoft Windows Server	2012 R2 Standard	Unmodified COTS	EMS Server SW Component
Microsoft Windows	10 Professional	Unmodified COTS	EMS Client/Server SW Component
.NET Framework	3.5	Unmodified COTS	EMS Client/Server SW Component
Microsoft Visual J#	2.0	Unmodified COTS	EMS Client/Server SW Component
Microsoft Visual C++ 2013 Redistributable	2013	Unmodified COTS	EMS Client/Server SW Component
Microsoft Visual C++ 2015 Redistributable	2015	Unmodified COTS	EMS Client/Server SW Component

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 46 of 61

System Component	Version	Operating System or COTS	Comments
Java Runtime Environment	7u80	Unmodified COTS	EMS Client/Server SW Component
Java Runtime Environment	8u144	Unmodified COTS	EMS Client/Server SW Component
Microsoft SQL Server 2016 Standard	2016 Standard	Unmodified COTS	EMS Client/Server SW Component
Microsoft SQL Server 2016 Service Pack 2	2016 SP1	Unmodified COTS	EMS Client/Server SW Component
Microsoft SQL Server 2016 SP1 Express	2016 SP2	Unmodified COTS	EMS Client/Server SW Component
Cepstral Voices	6.2.3.801	Unmodified COTS	EMS Client/Server SW Component
Arial Narrow Fonts	2.37a	Unmodified COTS	EMS Client/Server SW Component
Maxim iButton Driver	4.05	Unmodified COTS	EMS Client/Server SW Component
Adobe Reader DC	AcrobatDC	Unmodified COTS	EMS Client/Server SW Component
Microsoft Access Database Engine	2010	Unmodified COTS	EMS Client/Server SW Component
Open XML SDK 2.0 for Microsoft Office	2.0	Unmodified COTS	EMS Client/Server SW Component
Infragistics NetAdvantage Win Forms 2011.1	2011 Vol. 1	Unmodified COTS	EMS SW Platform
Infragistics NetAdvantage WPF 2012.1	2012 Vol. 1	Unmodified COTS	EMS SW Platform
TX Text Control Library for .NET	16.0	Unmodified COTS	EMS SW Platform
SOX	14.3.1	Unmodified COTS	EMS SW Platform
NLog	1.0.0.505	Unmodified COTS	EMS SW Platform
iTextSharp	5.0.5	Unmodified COTS	EMS SW Platform
OpenSSL	1.0.2K	Unmodified COTS	EMS SW Platform
OpenSSL FIPS Object Module	2.0.14	Unmodified COTS	EMS SW Platform
SQLite	1.0.103.0	Unmodified COTS	EMS SW Platform
Lame	3.99.4	Unmodified COTS	EMS SW Platform
Speex	1.0.4	Unmodified COTS	EMS SW Platform
Ghostscript	9.04	Unmodified COTS	EMS SW Platform
One Wire API for .NET	4.0.2.0	Unmodified COTS	EMS SW Platform
Avalon-framework-cvs-20020806	20020806	Unmodified COTS	EMS SW Platform
Batik	0.20-5	Unmodified COTS	EMS SW Platform
Fop	0.20-5	Unmodified COTS	EMS SW Platform
Microsoft Visual J# 2.0 Redistributable Package – Second Edition (x64)	2.0	Unmodified COTS	EMS SW Platform
Entity framework	6.1.3	Unmodified COTS	EMS SW Platform
Spreadsheetlight	3.4.3	Unmodified COTS	EMS SW Platform
Open XML SDK 2.0 for Microsoft Office	2.0.5022.0	Unmodified COTS	EMS SW Platform
Open SSL	1.0.2K	Unmodified COTS	ICP
OpenSSL FIPS Object Module	2.0.10	Unmodified COTS	ICP
Zlib	1.2.3	Unmodified COTS	ICP
uClinux	20070130	Modified COTS	ICP
Kernel (Linux)	2.6.30.9-dvs-36	Modified COTS	ICE

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 47 of 61

System Component	Version	Operating System or COTS	Comments
U-Boot	1.3.4	Modified COTS	ICE
Google Text-to-Speech Engine	3.11.12	Unmodified COTS	ICX SW
Kernel	4.9.11	Modified COTS	ICP2
U-Boot	2017.03	Modified COTS	ICP2
Zxing Barcode Scanner	4.7.5	Modified COTS	ICX SW
SoundTouch	1.9.2	Modified COTS	ICX SW
ICX Prime Android 5.1.1 Image	5.1.1-1.17.3	Modified COTS	ICX SW
ICX Classic Android 4.4.4 Image	0.0.98	Modified COTS	ICX SW
OpenSSL FIPS Object Module	2.0.10 (Cert 2473)	Unmodified COTS	ICX SW Build Library
OpenSSL	1.0.2K	Unmodified COTS	ICC SW Build Library
OpenSSL FIPS Object Module	2.0.10 (Cert 1747)	Unmodified COTS	ICC SW Build Library
1-Wire Driver (x86)	4.05	Unmodified COTS	ICC Runtime SW
1-Wire Driver (x64)	4.05	Unmodified COTS	ICC Runtime SW
Canon DR-G1130 TWAIN Driver	1.2 SP6	Unmodified COTS	ICC Runtime SW
Canon DR-G160II TWAIN Driver	1.2 SP6	Unmodified COTS	ICC Runtime SW
Canon DR-M260 TWAIN Driver,	1.1 SP2	Unmodified COTS	ICC Runtime SW
InoTec HiPro 821 TWAIN Driver	1.2.0.5	Unmodified COTS	ICC Runtime SW
Visual C++ 2013 Redistributable (x86)	12.0.30501	Unmodified COTS	ICC Runtime SW
Machine Configuration File (MCF)	5.5.15.1_20200306	Proprietary	ICX Configuration File
Device Configuration File (DCF)	5.5.41.3_20200507	Proprietary	ICP and ICC Configuration File
ICE Machine Behavior Settings	5.5.6.3_20200415	Proprietary	ICE Configuration
ICP2 Machine Behavior Settings	5.5.2.1_20200415	Proprietary	ICP2 Configuration

Hardware Components:

System Component	Hardware Version	Proprietary or COTS	Comments
ImageCast Precinct (ICP)	PCOS-320C	Proprietary	Precinct Scanner
ImageCast Precinct (ICP)	PCOS-320A	Proprietary	Precinct Scanner
ImageCast 2 Precinct (ICP2)	PCOS-330A	Proprietary	Precinct Scanner
ImageCast Evolution (ICE)	PCOS-410A	Proprietary	Precinct Scanner
ICP Ballot Box	BOX-330A	Proprietary	Ballot Box
ICP Ballot Box	BOX-340C	Proprietary	Ballot Box
ICP Ballot Box	BOX-341C	Proprietary	Ballot Box
ICP Ballot Box	ElectionSource IM-COLLAPSIBLE	Proprietary	Ballot Box
ICE Ballot Box	BOX-410A	Proprietary	Ballot Box
ICE Ballot Box	BOX-420A	Proprietary	Ballot Box
ICP2 Ballot Box	BOX-350A	Proprietary	Ballot Box
ICP2 Ballot Box	BOX-340C	Proprietary	Ballot Box
ICP2 Ballot Box	BOX-341C	Proprietary	Ballot Box
ICP2 Ballot Box	ElectionSource IM-COLLAPSIBLE	Proprietary	Ballot Box
ICX UPS Inline EMI Filter	1.0	Proprietary	EMI Filter
ICX Tablet (Classic)	aValue 15" Tablet (SID-15V)	COTS	Ballot Marking Device
ICX Tablet (Classic)	aValue 21" Tablet (SID-21V)	COTS	Ballot Marking Device
ICX Tablet (Prime)	aValue 21" Tablet (HID-21V) (Steel or Aluminum chassis)	COTS	Ballot Marking Device or Direct Recording Electronic
Thermal Printer	SII RP-D10	COTS	Report Printer

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 48 of 61

System Component	Hardware Version	Proprietary or COTS	Comments
Thermal Printer (VVPAT)	KFI VRP3 V1 and V1C	COTS	Voter-verifiable paper audit trail (VVPAT)
Server	Dell PowerEdge R620	COTS	Standard Server
Server	Dell PowerEdge R630	COTS	Standard Server
Server	Dell PowerEdge R640	COTS	Standard Server
ICC Workstation HW	Dell Optiplex 5270 All in One	COTS	
ICC Workstation HW	Dell OptiPlex 7440 All in One	COTS	
ICC Workstation HW	Dell OptiPlex 3050 All In One	COTS	
ICC Workstation HW	Dell OptiPlex 9030 All In One	COTS	
ICC Workstation HW	Dell OptiPlex 9020 All In One	COTS	
ICC Workstation HW	Dell OptiPlex 9010 All In One	COTS	
ICC Scanner	Canon imageFormula DR-G1130	COTS	Central Count Scanner
ICC Scanner	Canon imageFormula DR-M160II	COTS	Central Count Scanner
ICC Scanner	Canon imageFormula DR-M260	COTS	Central Count Scanner
ICC Scanner	Canon imageFormula DR-G2140	COTS	Central Count Scanner
ICC Scanner	InoTec HiPro 821	COTS	Central Count Scanner
ICC Scanner	Dell Optiplex 7070	COTS	
ICC Scanner	Dell Optiplex 7060	COTS	
ICC Scanner	Dell Optiplex 7050	COTS	
ICC Scanner Monitor	Lenovo 10QXPAR1US	COTS	
ICC Scanner Monitor	Dell 2418HT Monitor	COTS	
Client Workstation HW and Express Server	Dell Precision 3430	COTS	
Client Workstation HW and Express Server	Dell Precision 3431	COTS	
Client Workstation HW and Express Server	Dell Precision T3420	COTS	
Client Workstation HW	Dell Precision T1700	COTS	
Client Workstation HW	Dell Latitude 3400	COTS	
Client Workstation HW	Dell Latitude 3490	COTS	
Client Workstation HW	Dell Latitude E3480	COTS	
Client Workstation HW	Dell Latitude E3470	COTS	
Client Workstation HW	Dell Latitude E7450	COTS	
ICX Printer	HP LaserJet Pro Printer M402dn	COTS	
ICX Printer	HP LaserJet Pro Printer M402dne	COTS	
ICX Printer	HP LaserJet Printer M501dn	COTS	
ICE Dual Monitor	AOC e1649FWU	COTS	
ICE Dual Monitor	Display Logic LM15.6-USB-DV.B	COTS	
Monitor	Dell Monitor KM632	COTS	
Monitor	Dell Monitor P2414Hb	COTS	
Monitor	P2419H	COTS	
Monitor	P2417H	COTS	
Monitor	Dell Ultrasharp 24" Monitor U2414H	COTS	
CD/DVD Reader	Dell DVD Multi Recorder GP60NB60	COTS	
iButton Programmer	Maxim iButton Programmer DS9490R# with DS1402-RP8+	COTS	
UPS	Tripp Lite SMART1500RMXL2U	COTS	
UPS	APC SMT1500C Smart-UPS	COTS	
UPS	APC SMT1500 Smart-UPS	COTS	
UPS	APC BE600M1	COTS	
UPS	APC BR1000G	COTS	

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 49 of 61

System Component	Hardware Version	Proprietary or COTS	Comments
UPS	CyberPower PR1500LCD	COTS	
UPS	CyberPower PR1500LCD-VTVM	COTS	
Network Switch	Dell X1008	COTS	
Network Switch	Dell X1018	COTS	
Network Switch	Dell X1026	COTS	
Network Switch	Dell PowerConnect 2808	COTS	
Sip and Puff	Enabling Devices #972	COTS	
Headphones	Cyber Acoustics ACM-70 and ACM-70B	COTS	
4-way Joystick Controller	S26	Modified COTS	
Rocker (Paddle) Switch	Enabling Device #971	COTS	
Rocker (Paddle) Switch	AbleNet 10033400 (2x)	COTS	
Rocker (Paddle) Switch Cable	Hosa Technology YMM-261 (for use with AbleNet switches)	COTS	
CF Card Reader	IOGEAR SDHC/microSDHC 0U51USC410	COTS	
CF Card Dual-Slot Reader	Lexar USB 3.0	COTS	
CF Card Reader	Hoodman Steel USB 3.0 102015	COTS	
CF Card Reader	Lexar Professional CFR1	COTS	
CF Card Reader	Kingston FCR-HS4	COTS	
ATI	ATI handset	Proprietary	
ATI	ATI-USB handset	Proprietary	
ACS PC-Linked Smart Card Reader	ACR38U	COTS	
ACS PC-Linked Smart Card Reader	ACR39U	COTS	

System Limitations

This table depicts the limits the system has been tested and certified to meet.

Characteristic	Limiting Component	Limit	Comment
Ballot positions	22" Ballot	292*/462**	Landscape Ballot: 240 candidates + 24 write-ins + 28 Yes/No choices.
Precincts in an election	EMS	1000; 250	Memory Standard; Express
Contests in an election	EMS	1000; 250	Memory Standard; Express
Candidates/Counters in an election	EMS	10000; 2500	Memory Standard; Express
Candidates/Counters in a precinct	22" Ballot	240*/462**	Memory Both EMS
Candidates/Counters in a tabulator	Tabulator	10000; 2500	Memory Standard; Express
Ballot Styles in an election	Tabulator	3000; 750	Memory Standard; Express
Ballot IDs in a tabulator	ICP	200	Memory Both EMS
Contests in a ballot style	ICX BMD Ballot	38*/156**	14" Ballot Both EMS
Candidates in a contest	22" Ballot	240*/231**	Ballot Both EMS
Ballot styles in a precinct	Tabulator	5	Memory Both EMS
Number of political parties	Tabulator	30	Memory Both EMS
"vote for" in a contest	22" Ballot	24*/30**	Ballot Both EMS
Supported languages in an election	Tabulator	5	Memory Both EMS

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 50 of 61

Characteristic	Limiting Component	Limit	Comment
Number of write-ins	22 "Ballot	24*/462**	Ballot Both EMS

* Reflects the system limit for a ballot printed in landscape.

** Reflects the system limit for a ballot printed in portrait.

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 51 of 61

Functionality

2005 VVSG Supported Functionality Declaration

Feature/Characteristic	Yes/No	Comment
Voter Verified Paper Audit Trails		
VVPAT	YES	
Accessibility		
Forward Approach	YES	
Parallel (Side) Approach	YES	
Closed Primary		
Primary: Closed	YES	
Open Primary		
Primary: Open Standard (provide definition of how supported)	YES	
Primary: Open Blanket (provide definition of how supported)	YES	
Partisan & Non-Partisan:		
Partisan & Non-Partisan: Vote for 1 of N race	YES	
Partisan & Non-Partisan: Multi-member ("vote for N of M") board races	YES	
Partisan & Non-Partisan: "vote for 1" race with a single candidate and write-in voting	YES	
Partisan & Non-Partisan "vote for 1" race with no declared candidates and write-in voting	YES	
Write-In Voting:		
Write-in Voting: System default is a voting position identified for write-ins.	YES	
Write-in Voting: Without selecting a write in position.	NO	
Write-in: With No Declared Candidates	YES	
Write-in: Identification of write-ins for resolution at central count	YES	
Primary Presidential Delegation Nominations & Slates:		
Primary Presidential Delegation Nominations: Displayed delegate slates for each presidential party	YES	
Slate & Group Voting: one selection votes the slate.	YES	
Ballot Rotation:		
Rotation of Names within an Office; define all supported rotation methods for location on the ballot and vote tabulation/reporting	YES	Equal time rotation
Straight Party Voting:		
Straight Party: A single selection for partisan races in a general election	YES	
Straight Party: Vote for each candidate individually	YES	
Straight Party: Modify straight party selections with crossover votes	YES	
Straight Party: A race without a candidate for one party	YES	
Straight Party: "N of M race (where "N">1)	YES	
Straight Party: Excludes a partisan contest from the straight party selection	YES	
Cross-Party Endorsement:		

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 52 of 61

Feature/Characteristic	Yes/No	Comment
Cross party endorsements, multiple parties endorse one candidate.	YES	
Split Precincts:		
Split Precincts: Multiple ballot styles	YES	
Split Precincts: P & M system support splits with correct contests and ballot identification of each split	YES	
Split Precincts: DRE matches voter to all applicable races.	YES	
Split Precincts: Reporting of voter counts (# of voters) to the precinct split level; Reporting of vote totals is to the precinct level	YES	
Vote N of M:		
Vote for N of M: Counts each selected candidate, if the maximum is not exceeded.	YES	
Vote for N of M: Invalidates all candidates in an overvote (paper)	YES	
Recall Issues, with options:		
Recall Issues with Options: Simple Yes/No with separate race/election. (Vote Yes or No Question)	YES	
Recall Issues with Options: Retain is the first option, Replacement candidate for the second or more options (Vote 1 of M)	NO	
Recall Issues with Options: Two contests with access to a second contest conditional upon a specific vote in contest one. (Must vote Yes to vote in 2nd contest.)	NO	
Recall Issues with Options: Two contests with access to a second contest conditional upon any vote in contest one. (Must vote Yes to vote in 2nd contest.)	NO	
Cumulative Voting		
Cumulative Voting: Voters are permitted to cast, as many votes as there are seats to be filled for one or more candidates. Voters are not limited to giving only one vote to a candidate. Instead, they can put multiple votes on one or more candidate.	NO	
Ranked Order Voting		
Ranked Order Voting: Voters can write in a ranked vote.	NO	
Ranked Order Voting: A ballot stops being counting when all ranked choices have been eliminated	NO	
Ranked Order Voting: A ballot with a skipped rank counts the vote for the next rank.	NO	
Ranked Order Voting: Voters rank candidates in a contest in order of choice. A candidate receiving a majority of the first choice votes wins. If no candidate receives a majority of first choice votes, the last place candidate is deleted, each ballot cast for the deleted candidate counts for the second choice candidate listed on the ballot. The process of eliminating the last place candidate and recounting the ballots continues until one candidate receives a majority of the vote	NO	
Ranked Order Voting: A ballot with two choices ranked the same, stops being counted at the point of two similarly ranked choices.	NO	

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 53 of 61

Feature/Characteristic	Yes/No	Comment
Ranked Order Voting: The total number of votes for two or more candidates with the least votes is less than the votes of the candidate with the next highest number of votes, the candidates with the least votes are eliminated simultaneously and their votes transferred to the next-ranked continuing candidate.	NO	

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 54 of 61

Feature/Characteristic	Yes/No	Comment
Provisional or Challenged Ballots		
Provisional/Challenged Ballots: A voted provisional ballots is identified but not included in the tabulation, but can be added in the central count.	YES	
Provisional/Challenged Ballots: A voted provisional ballots is included in the tabulation, but is identified and can be subtracted in the central count	NO	
Provisional/Challenged Ballots: Provisional ballots maintain the secrecy of the ballot.	YES	
Overvotes (must support for specific type of voting system)		
Overvotes: P & M: Overvote invalidates the vote. Define how overvotes are counted.	YES	Overvotes cause a warning to the voter and can be configured to allow voter to override.
Overvotes: DRE: Prevented from or requires correction of overvoting.	YES	
Overvotes: If a system does not prevent overvotes, it must count them. Define how overvotes are counted.	YES	If allowed via voter override, overvotes are tallied separately.
Overvotes: DRE systems that provide a method to data enter absentee votes must account for overvotes.	N/A	
Undervotes		
Undervotes: System counts undervotes cast for accounting purposes	YES	
Blank Ballots		
Totally Blank Ballots: Any blank ballot alert is tested.	YES	Precinct voters receive a warning; both precinct and central scanners will warn on blank ballots.
Totally Blank Ballots: If blank ballots are not immediately processed, there must be a provision to recognize and accept them	YES	Blank ballots are flagged. These ballots can be manually examined and then be scanned and accepted as blank; or precinct voter can override and accept.
Totally Blank Ballots: If operators can access a blank ballot, there must be a provision for resolution.	YES	Operators can examine a blank ballot, re-mark if needed and allowed, and then re-scan it.
Networking		
Wide Area Network – Use of Modems	NO	
Wide Area Network – Use of Wireless	NO	

Exhibit 1

Petition for Approval of Electronic Voting Systems
 Democracy Suite 5.5-C and 5.5-CS
 June 2, 2021
 Page 55 of 61

Feature/Characteristic	Yes/No	Comment
Local Area Network – Use of TCP/IP	YES	Client/server only
Local Area Network – Use of Infrared	NO	
Local Area Network – Use of Wireless	NO	
FIPS 140-2 validated cryptographic module	YES	
Used as (if applicable):		
Precinct counting device	YES	ImageCast Precinct ImageCast Precinct 2 ImageCast Evolution ImageCast X DRE
Central counting device	YES	ImageCast Central

Baseline Certification Engineering Change Orders (ECO)

ECO #	Component	Description
100607	ImageCast Central - HiPro Scanner configuration	Added Dell Optiplex 7060 and 7070.
100653	ImageCast Central Scanner Workstation	Added DELL Optiplex 5270 AIO computer.
100624	ImageCast Evolution	Alternative supplier (King Cord) for ICE power cord
100648	ImageCast Precinct 2	Added new Centon SDHC memory device"
100630	ImageCast Central	Added a scanner (Canon DR-G2140) for use with the D-Suite ImageCast Central workstation
100654	ImageCast Precinct2 PCOS 330A	Adding the ICP2 adapter plate for use with Eagle ballot box
100657	ImageCast Evolution PCOS 410A	Added Addmaster KR-85A printer as an AVL replacement
100669	ImageCast X Prime	Added RRC 2054-2 battery as an AVL for the ICX Prime replacement battery.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 56 of 61

Appendix F: Voting System Standards, Testing Protocols and Procedures Pertaining to the Use of Communication Devices

PART I: PROPOSED TESTING STANDARDS

Applicable VVSG Standard

The 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. Meeting the requirements contained in the VVSG may substantiate compliance with the voting system requirements contained in Section 301 of the Help America Vote Act of 2002 (HAVA).

Access to Election Data

Provisions shall be made for authorized access to election results after closing of the polls and prior to the publication of the official canvass of the vote. Therefore, 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. The system may be designed so that results may be transferred to an alternate database or device. 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.

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.

Accuracy

A voting system must be capable of accurately recording and reporting votes cast. Accuracy provisions shall be evidenced by the inclusion of control logic and data processing methods, which incorporate parity, and checksums, or other equivalent error detection and correction methods.

Data Integrity

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 57 of 61

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. These provisions shall include protection against:

- the interruption of electrical power, generated or induced electromagnetic radiation.
- ambient temperature and humidity.
- the failure of any data input or storage device.
- any attempt at an improper data entry or retrieval procedure.

Reliability

Successful Completion of the Logic and Accuracy test shall be determined by two criteria

- The number of failures in transmission
- and the accuracy of vote counting

The failure or connectivity rate will be determined by observing the number of relevant failures that occur during equipment operation. The accuracy is to be measured by verifying the completeness of the totals received.

PART II: TEST PROCEDURES AND PROTOCOLS

Overview of Telecommunication Test

The telecommunication test focuses on system hardware and software function and performance for the transmission of data that is used to operate the system and report election results. This test applies to the requirements for Volume I, Section 6 of the EAC 2005 VVSG. This testing is intended to complement the network security requirements found in Volume I, Section 7 of the EAC 2005 VVSG, which include requirements for voter and administrator access, availability of network service, data confidentiality, and data integrity. Most importantly, security services must restrict access to local election system components from public resources, and these services must also restrict access to voting system data while it is in transit through public networks. Compliance with Section 7, EAC 2005 VVSG shall be evidenced by a VSTL report submitted with the vendor's application for approval of a voting system.

In an effort to achieve these standards and to verify the proper functionality of the units under test, the following methods will be used to test each component of the voting system:

Wired Modem Capability Test Plan

Test Objective: To transfer the results from the tabulator to the Election Management System via a wired network correctly.

Test Plan:

1. Attempt to transmit results prior to the closing of the polls and printing of results tape

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 58 of 61

2. Set up a telephone line simulator that contains as many as eight phone lines
3. Perform communication suite for election night reporting using a bank with as many as seven analog modems:
 - a. Connect the central site election management system to the telephone line simulator and connect the modems to the remaining telephone line ports
 - b. Setup the phone line numbers in the telephone line simulator
 - c. Use the simulated election to upload the election results
 - i. Use at least eight tabulators in different reporting units
 - ii. Use as many as two tabulators within the same reporting units
 - d. Simulate the following transmission anomalies
 - i. Attempt to upload results from a tabulating device to a computer which is not part of the voting system
 - ii. Attempt to upload results from a non-tabulating device to the central site connected to the modem bank
 - iii. Attempt to load stress by simulating a denial of service (DOS) attack or attempt to upload more than one polling location results (e.g., ten or more polling locations)

Wireless Capability Test Plan

Test Objective: To transfer the results from the tabulator to EMS via a wireless network correctly.

Test Plan:

1. Attempt to transmit results prior to the closing of the polls and printing of results tape.
2. Perform wireless communication suite for election night reporting:
 - a. Use the simulated election to upload the election results using wireless transfer to the secure FTP server (SFTP)
 - b. Use at least eight tabulators in different reporting units
 - c. Use as many as two tabulators within the same reporting unit
3. Simulate the following transmission anomalies
 - a. Attempt to upload results from a tabulating device to a computer which is not part of the voting system
 - b. Attempt to upload results from a non-tabulating device to the SFTP server
 - c. Attempt to load stress by simulating a denial of service (DOS) attack or attempt to upload more than one polling location results (e.g., ten or more polling locations)
 - d. If possible, simulate a weak signal
 - e. If possible, simulate an intrusion

Test Conclusions for Wired and Wireless Transmission

- System must be capable of transferring 100% of the contents of results test packs without error for each successful transmission.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 59 of 61

- Furthermore, system must demonstrate secure rate of transmission consistent with security requirements.
- System must demonstrate the proper functionality to ensure ease of use for clerks on election night.
- System must be configured such that the modem component remains inoperable until after the official closing of the polls and printing of one (1) copy of the results tape.

PART III: PROPOSED SECURITY PROCEDURES

Staff recommends that as a condition of purchase, any municipality or county which purchases this equipment and uses modem functionality must also agree to the following conditions of approval.

1. Devices which may be incorporated in or attached to components of the system for the purpose of transmitting tabulation data to another data processing system, printing system, or display device shall not be used for the preparation or printing of an official canvass of the vote unless they conform to a data interchange and interface structure and protocol which incorporates some form of error checking.
2. Any jurisdiction using a modeming solution to transfer results from the polling place to the central count location may not activate the modem functionality until after the polling place closes.
3. Any municipality using modeming technology must have one set of results printed before it attempts to modem any data.
4. Any municipality purchasing and using modem technology to transfer results from the polling location to the central count location must conduct an audit of the voting equipment after the conclusion of the canvass process.
5. Default passwords provided by DVS to county/municipality must be changed upon receipt of equipment.
6. Counties must change their passwords after every election.

PART IV: CONDITIONS FOR APPROVAL (VENDOR)

Additionally, staff recommends that, as a condition/continuing condition of approval, DVS shall:

1. Reimburse actual costs incurred by the WEC, and local election officials, where applicable, in examining the system (*including travel and lodging*) pursuant to state processes.
2. Configure modem component to remain inoperative (incapable of either receiving or sending transmissions) prior to the closing of the polls and the printing of tabulated results.

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 60 of 61

APPENDIX G: Wisconsin Voting Equipment Review Panel's Feedback

These comments were provided via a structured feedback form.

1. How would you rate the functionality of the equipment?

Extremely Poor	Poor	Fair	Good	Excellent
	1		2	2

- I ranked the functionality of the equipment as “poor” because of how the accessibility features of the Dominion ICE machine function. The way the system is set up, a voter wanting to use the accessible features of the equipment has to have additional contact with the poll workers that other voters are not required to do. It also required additional training of poll workers to ensure they understood how to use the magnetic key. Also of note the ballot is printed using the ICX ballot marking device is clearly different from the ballots any other voter produces, as it has a QR code on it. This fact limits the ballot privacy for voters who make use of the ballot marking device. There is no way for the voter to double check the data encoded in the QR code before putting the ballot into the tabulator. This functionality is available in other equipment such as the ES&S ExpressVote. If this equipment would ever be tabulated by a machine rather than solely by hand count, I would recommend considering adding that functionality.
- Would like better sorting system on central scanner
- Report of write-ins is nice.
- Functionality of the equipment is good. Streamlined features seem to make seem to make tabulating and voting easier. Worry re: QR code and inability to read back to the voter.

2. How would you rate the accessible features?

Extremely Poor	Poor	Fair	Good	Excellent
1			1	3

- I was impressed with the variety of options that were available in terms of accessible equipment. I could see a potential line issue with the equipment that is accessible and a tabulator (please forgive me for not having the model number, it was the first item that was demonstrated) if someone is using the accessible portion while others want to simply tabulate a ballot.
- The dual nature of the Dominion ImageCast Evolution presents challenges for voters with and without disabilities. The tabulator can be converted into a touch screen machine, but that requires that the machine be temporarily closed for use by voters who wanted to submit their ballots. This can be very intimidating for a voter with a disability to have to try and vote using the accessibility functionality while a line of voters wanting to put their ballots into the machine starts to form behind them. The dual nature of the machine also

Exhibit 1

Petition for Approval of Electronic Voting Systems
Democracy Suite 5.5-C and 5.5-CS
June 2, 2021
Page 61 of 61

means that it is not readily identifiable as the accessible voting equipment by voters and poll workers with limited training, so voters who need to use the accessible features may not know it is available for them to use. Please consider requiring jurisdictions to acquire and set up the external screen as part of the certification requirements to use this equipment. This would address some of the biggest issues with the equipment.

- Unable to verify QR code to see if it is reading correct selections
- Accessibility features seem streamlined and allow for voters to cast a ballot privately and independently. Ability for voters to bring in own equipment is important.

3. Rate your overall impression of the system.

Extremely Poor	Poor	Fair	Good	Excellent
	1		2	2

- As previously mentioned, my biggest concerns with the equipment is the dual nature of the Dominion ICE machine. In practice it check the box of accessibility, but is not truly accessible in practice.
- We do use the equipment county wide. We continuously receive positive comments from voters that the system is easy to use. The election officials also report that the equipment is easy to use from their end. After the April 2021 election, there were 2 recounts requested. One of the contests was a 1-point difference. When the recount was completed, the vote remained the same. The second recount was a 17-point difference. Again, no vote difference. However, “unintentional” human errors that training will again need to be addressed.
- Variations in types of machines to best suit polling places and community needs.

Exhibit 1