SUBPOENA

THE STATE OF WISCONSIN

TO CLERK PATRICK W. MOYNIHAN, JR.

BROWN COUNTY CLERK

NORTHERN BUILDING

305 E WALNUT STREET, ROOM 120

GREEN BAY, WI 54301

PURSUANT TO WIS. STATS. 885.01 (4) AND 2021 ENROLLED ASSEMBLY RESOLUTION 15 DATED MARCH 23, 2021, YOU ARE HEREBY ORDERED TO APPEAR BEFORE THE ASSEMBLY CAMPAIGNS AND ELECTIONS COMMITTEE AT A COUNTY FACILITY OF YOUR CHOOSING ON THE 7TH DAY OF SEPTEMBER, 2021 AT NOON OF THAT DAY, TO GIVE EVIDENCE IN THE MATTER OF THE 2020 PRESIDENTIAL GENERAL ELECTION THEN AND THERE TO BE HEARD. FAILURE TO APPEAR MAY RESULT IN PUNISHMENT FOR CONTEMPT, WHICH MAY INCLUDE MONETARY PENALTIES, IMPRISONMENT AND OTHER SANCTIONS.

YOU ARE FURTHER REQUIRED TO BRING WITH YOU THE FOLLOWING DOCUMENTATION AND ITEMS DETAILED IN THE ATTACHED EXHIBIT A.

GIVEN UNDER MY HAND THIS 6TH DAY AUGUST, 2021.

JANEL BRANDTJEN, CHAIR

ASSEMBLY CAMPAIGNS & ELECTIONS COMMITTEE

Exhibit A – Cyber Forensic Audit

Pertaining to the November 2020 General Election, the Assembly's Campaigns & Elections Committee requests access to the following books, letters, or other documentary evidence from your county for the purpose of forensic analysis:

1. The physical ballots in the November 2020 election, 100% of the mail-in ballots, provisional ballots, and physical ballots cast in person the day of the election.

2. All ballot production, processing, and tabulation equipment from satellite election offices and any other location used to count votes.

3. The software and bootable media, hardware tokens (security keys) for the equipment described in item #1, and the election management system that was used.

4. Forensic images of all election equipment:

- Servers – Election management server, file servers, network servers, dial-up servers, or any other server utilized for the processing or storage of election results or data required to run an election.
- Tabulators – high speed and normal speed
- Ballot marking devices – including accessibility, or for normal voting
- Desktops & laptops – Utilized within the Election Management System for any purpose including but not limited to: EMS Client, adjudication, registration, creation of ballots or designs, processing results, uploading results or anything similar
- Signature matching and ballot sorting equipment
- Switches, routers or other network equipment – This includes normal networking equipment as well as any specialized systems such as Intrusion Detection Systems, Firewalls, Intrusion Prevention Systems or similar

5. Forensic images of all removable media (including, but not limited to USB thumb drives, external hard drives, backup tape cassettes, memory cards, PCMIA cards, Compact Flash, CD/DVD or similar) used as part of the election process or to load software, configuration, or programming.

6. Forensics images of the firmware of any device associated with the election that does not have a hard drive; including any tooling required to extract that firmware, if applicable.

7. Forensic images of all SIM cards used for wireless 3G/4G LTE/5G communications.

8. Forensics on all machines utilized for absentee ballot processing to include:

- All logs from the system
- Backups of the system
- Offsite cloud storage associated with the system
- Media used to transfer data (USB drives, compact flash, external hard drives)

9. Logs from all routers, switches, firewalls, IDS, IPS or similar devices. This includes, but is not limited to:

- Netflows (or equivalent)
- DHCP logs
- Access logs
- VPN logs
- PPP logs
- RDP logs
- Splunk logs
- Any remote administration tool logs

10. Logs from all computer systems, servers, desktops, laptops, or similar including but not limited that were used in the design, management, and running of the election:

- Windows Event logs
- Access logs
- Firewall logs
- IDS / IPS / Malware / Virus Scan Logs
- Database logs
- All logs generated from applications associated in any way with the election

11. Logs from all EMS Server(s), EMS Clients, tabulators, ballot marking devices, ballot on demand printers, scanners, voting systems, or other election equipment including, but not limited to:

- Error logs
- Access logs
- Debug output
- Audit logs
- Administrator logs

12. Election Log Files XML, EML, JSON, DVD and XSLT other election files and logs for:

- Tabulators
- Result pair resolution
- Result files
- Provisional votes
- RTM logs
- SQL database files and logs
- Signature checking & sorting machine

13. List of all IP addresses utilized at any location where election equipment was utilized during the entire election period. This includes the time from when the election equipment was ready to receive a cast ballot to when the certified results were officially published. This shall include, but is not limited to:

- IP addresses of any cellular modems utilized by voting equipment
- IP addresses of any routers utilized at any location where votes were cast, counted, tallied, or reported

- IP addresses of any dial-up connections utilized
- IP addresses of any computers utilized to process, send or upload election results

14. Access or control of ALL routers, tabulators or combinations thereof (some routers are inside the tabulator case) in order to gain access to all the system logs.

15. Election Settings:

- Ranked profiles and entire change history of audit trail logs
- Ranked contests and entire change history audit trail logs
- Rejected ballots report by reason code
- All configuration files utilized to control the election

16. Accounts and Tokens:

- Username & Passwords (Applications, Operation Systems, Routers, Switches, Firewalls, etc)
- File and/or Hardrive Encryption Passwords or keys (Bitlocker, Veracrypt, Etc)
- Security Tokens (iButton, Yubikey, SmartCard, Etc)

17. ES&S Express VoteXL Specific:

- All Paper Vote Summary Cards
- All USB Flash Drives

18. Voter Rolls:

- Database of voter rolls
- Forensic Image of computer/device used to work with voter rolls
- Copy of media device used to transfer voter rolls

19. Records required from the voting system- Daily and cumulative voter records for those who voted with sufficient definition to determine:

- Voter's name and Registered Voting address
- Address for correspondence (mailing address)
- D.O.B.
- Voter ID number
- How Voted (mail, in-person early, in person Election Day)
- Where Voted (if applicable)
- Date voted (if applicable)
- Ballot by mail Request Date
- Ballot by mail sent date
- Ballot by mail voted date (if applicable)
- Ballet cancelled date (if applicable)
- RAW, HTML, XHTML and SVG files (Ballot Images)

20. Access needed to physically and forensically examine all date and time-stamped paper ballots as required:

- Voter Tally Paper Rolls, Test Ballots, Ballot Test Matrix

21. Paper samples from all ballot paper utilized during the 2020 election cycle.

22. All physical ballots cast or attempted to cast during the 2020 General Election. This includes, but is not limited to:

- Mail in and absentee ballots
- Provisional Ballots
- Early Voting Ballots
- Accessibility Ballots
- Spoiled Ballots
- UOCAVA ballots
- Election Day Ballots

23. All request forms for mail ballots and absentee ballots.

24. All envelopes for mail in and absentee ballots.

25. All reports detailing all ballots that were rejected prior to election day and the process to contact the voter to cure the ballot.

26. All cartridges from all voting machines and scanners.

27. All affidavits for assistance.

28. All envelopes of requested ballots that were returned as undeliverable.

29. All training materials used to train County Employees including temporary employees, Judges of Election, Inspectors, Clerks, and all persons who staffed the satellite voting offices.

30. All duplicated ballots and all logs that would allow the duplicate to be compared to the original.

31. Chain of custody records and procedures for all ballots from the start of the election through the current date.

32. All pollbooks from all wards and divisions.

33. All supplemental pollbooks from all wards and divisions.

34. A list of all voters who cast an absentee or mail ballot and voted on the machines at the polls on Election Day.

35. All contracts and agreements between the Brown County, including all departments under the direction of the mayor, and election vendors.

36. All contracts and agreements between any vendor or contractor that supplies voting equipment of any type, software utilized in the election process, ballot paper, election design support, election equipment support, or election support. This includes, but is not limited to contracts dealing with:

- Ballot Marking Devices, Tabulators, Election Management Systems, or similar
- Election Design Software, Tabulation Software, Voting Registration Software, Duplication Software, Adjudication Software, Signature Verification Software, or anything similar related to the election
- Ballot Paper, Printing Services, Mailing Services, Scanning Services, Address Validation Services
- Election Design Services, Election Equipment Repair, Election Equipment Service, Election Processing, or other Election support services
- Internet service provider, cellular service provider

37. Timeline (1 month prior to the election to 1 month after the election) for each location that utilized a piece of election equipment that includes:

- Who accessed the equipment (the organization they represent and their position in the organization), on what date, for what purpose, what electronic media was used, and what records were kept
- Any tests that were performed during the access of the equipment (voters on election day are not to be included)

38. A complete end-to-end election setup for use:

- This would include all the equipment necessary to simulate an election and recreate the precise scenarios of election day in 2020
- Central Server, tabulators (high speed and normal), poll pads, etc.
    - This specifically includes all of the passwords, security tokens, physical keys, key fobs, etc., needed to use each piece of equipment
- Instruction manuals on how to use the end-to-end setup
- Duplicate copy of election tabulator bootable media for multiple selected locations
- Ballots used in the locations selected

39. All wards return sheets with the paper tapes:

- Any return sheets that were unusable, needed to be recreated, or fixed in somehow should also be included with their notes (front and back)

40. Dates/times of the technicians/people of LAT testing that had access to election equipment.

41. Dates/times of software updates on election computers and servers.

42. Dates/times of certification of the equipment (servers, election computers, election hardware devices).

43. Details of all CTCL related activities, included but not limited to:

- Equipment purchased by CTCL
- Number and locations of drop boxes installed
- List of resources CTCL had access to, including voter rolls or other data

44. Details and data surrounding the WisVote/ERIC system including:

- A full copy of the database holding all records and change records in the WisVote/ERIC system
- A copy of all logs showing all changes to the voter rolls as well as the username, name, IP address, or other details of the individual making the change
- A list of individuals and organizations with access to the WisVote/ERIC system and any of its Application Programming Interfaces
- Manuals and programmer documentation for interfacing with the WisVote/ERIC system

45. List of where the clerk stores all election equipment and data along with list of individuals that have access to these areas.

46. Information related to voting system design, architecture, and configuration.

47. Information pertaining to cybersecurity protocols and settings put into place.