Full Forensic Audit Subpoena List

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

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

3. 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

4. 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.

5. 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

6. Forensic images of all SIM cards used for wireless 3G/4G LTE/5G communications (REASON: Some tabulators are configured with cellular cards that connect to the internet and if not properly configured could be remotely accessed.)

7. 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)

8. 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

9. Logs from all computer systems, servers, desktops, laptops or similar including but not limited that was 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

10. 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

11. 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

12. 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.

13. 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.

14. Election Settings

- Ranked Profiles and entire change history 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.

15. 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)

16. ES&S Express VoteXL Specific

- All Paper Vote Summary Cards
- All USB Flash Drives

17. 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

18. The following records shall be 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)
- Party affiliation (if recorded)
- 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)

19. 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

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

21. All 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 (REASON – if someone has received a mail ballot – were they properly required to turn it in to spoil before voting on machine)

- UOCAVA ballots
- Election Day Ballots

22. All request forms for mail ballots and absentee ballots

23. All envelopes for mail in and absentee ballots

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

25. All cartridges from all voting machines and scanners

26. All affidavits for assistance

28. 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

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

30. Chain of custody records and procedures for all ballots from the start of the election through the current date REASON: How did the ballots get from ballot drop boxes and satellite election offices? How many hands touched them?

31. All pollbooks from all precincts, wards, and divisions

32. All supplemental pollbooks from all precincts, wards and divisions

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

34. All contracts and agreements between the Philadelphia Commissioners Office and the City of Philadelphia Office of Innovation and Technology

35. All contracts and agreements between the Philadelphia Commissioners Office and the City of Philadelphia Office of the Managing Director

36. All contracts and agreements between the Philadelphia Commissioners Office and the City of Philadelphia Office of the Mayor including all Departments under the direction of the Mayor

37. 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.

38. 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)

39. A complete end-to-end election setup for use in a laboratory

- 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.

o 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.

40. All precincts 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)

41. Dates/Times of the technicians/people of LAT testing had access to election equipment.

42. Dates/Times of software updates on election computers and serves.

43. Dates/Times of certification of the equipment (servers, election computers, election hardware devices)

44. 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

45. Details and data surrounding the SURE system including:

- A full copy of the database holding all records and change records in the SURE 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 SURE system, any of its Application Programming Interfaces
- Manuals and programmer documentation for interfacing with the SURE system

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

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

48. Cyber security protocols put into place