Electronic Pollbook Pilot

OBJECTIVE

ELECT will evaluate the use of wireless connectivity in the operation of electronic pollbooks (EPBs) on Election Day to confirm that EPBs certified to the new standards can operate successfully while connected to the VPN or Cloud.

Goals:

- Assess feasibility of a statewide plan to connect EPBs on Election Day.
- Identify challenges and possible security concerns in allowing connectivity.
- Create guidance that identifies issues and regulates the use of wireless connectivity of EPBs on Election Day.

BACKGROUND

In the Commonwealth of Virginia, localities have over 8,000 pollbooks supported by three vendors. These vendors are: Knowink, Dem Tech, and Robis Elections. Virginia is one of thirteen states that certify electronic pollbooks. [1]In 2020, the Virginia Voting Systems Certification Standards were reviewed, updated, and approved by the State Board of Elections (SBE). The Commonwealth's new standards were directed at the internal and external security of the voting systems and electronic pollbooks. The new certification standards require EPBs to have a list of security-related requirements as a part of their solution for managed connectivity to/from locality devices. EPBs were also required to:

- Utilize security best practices for internet connectivity, including network, wireless and cloud service.
- Confirm that the connection or VPN must be FIPS 104-2 certified. Localities must ensure their certification by validating their credentials through their third party certification provider.

These new requirements allow for secure connectivity on Election Day. As of July 2021, all EPBs were certified to the new standards.

History:

ELECT began allowing EPBs to connect to the VPN or Cloud at satellite early voting sites during the 2020 General Election. EPBs that were used in past elections for check-in at satellite locations had to be certified to the new standards in order to meet the additional security requirements for connecting to the VPN or the Cloud. General Registrars, who opted into this, reported liking "faster and more accurate" data. Localities saw the following benefits:

[1] National Council of State Legislatures, Electronic Pollbooks, https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx

- EPB check-in times were much faster than with VERIS.
- General Registrars were able to view the voting status of the early-voting sites from their offices.
- Officers of Elections could check-in voters at the curbside.
- Accurate, real-time information allowed for the updating of voter records into VERIS to occur automatically and not manually.
- Command Center could monitor voter turnout in real-time.
- Command Center could monitor any technical issues related to units, such as being unplugged and running on low-battery, or issues related to pollworker logins.
- Command Center could "chat" with pollworkers to quickly troubleshoot any issues that arose with ease of communication.

Wireless connectivity at satellite early voting sites has now been tested during two elections, including the 2021 Democratic Primary and the 2020 General Election, without incident.

DESIGN

With successful wireless connectivity at satellite early voting sites, ELECT has enough assurance to move forward with allowing a limited number of localities to test their connectivity to the VPN or Cloud on Election Day. The Code of Virginia does not prohibit EPBs from connecting to the VPN or Cloud on Election Day but it does prohibit voting machines. Voting systems, which include voting machines, are best described as the electronic voting and counting machines used during an election and includes direct recording electronic machines (DRE) and ballot scanner machines.[2] While §24.2-625.2 of the Code of Virginia states that "there shall be no wireless communications on Election Day, while the polls are open, between or among *voting machines* within the polling place…" the section goes on to say that the provisions of the section "shall not be construed to prohibit the operation of electronic pollbook devices at polling places on election day."[3] Statutorily there are no hurdles or justification needed for expanding EPB connectivity to include Election Day; however, more information is needed to develop best practices and regulations moving forward to ensure the integrity of this process. ELECT has selected five localities to participate in a pilot project to test the use of electronic pollbook connectivity on Election Day.

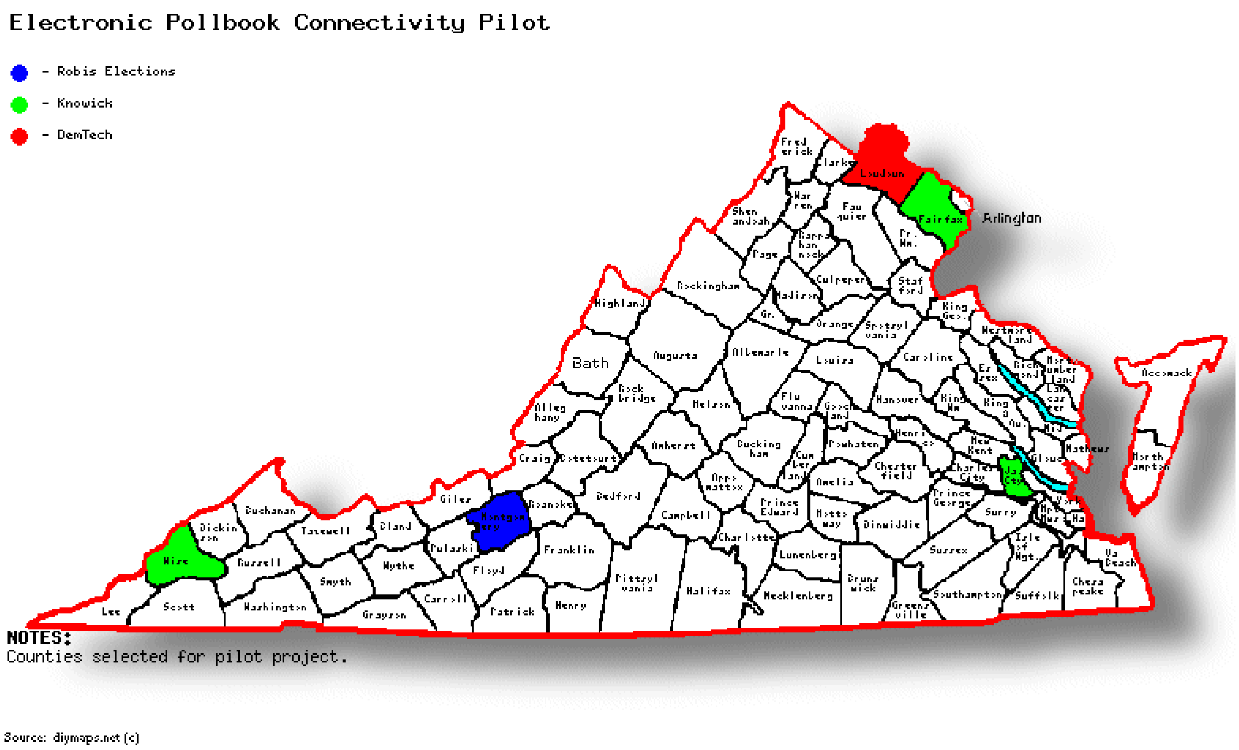
Participants:

Five localities have been selected for this project based on: size, vendor, geographical location, and interest in the project. Localities will be notified by email of their participation. They will be given a copy of the pilot plan. They will also receive a follow-up phone call to discuss any potential concerns or issues with the project.

All three certified vendors (Robis, Knowink, and DemTech) will be represented in the pilot. The localities that have been selected include: Wise, Fairfax, James City, Loudoun and Montgomery counties and are illustrated in the graphic below:

[2] Code of Virginia, §24,2-101 Definitions, https://law.lis.virginia.gov/vacode/24.2-101/

[3] Code of Virginia, §24.2-625.2, https://law.lis.virginia.gov/vacode/title24.2/chapter6/section24.2-625.2/


Electronic Pollbook Connectivity Pilot

● - Robis Elections

● - Knowick

● - DemTech

NOTES:
Counties selected for pilot project.

Source: diymaps.net (c)

VENDOR	LOCALITY	NUMBER OF REG. VOTERS
Knowink	Fairfax County	765,000
DemTech	Loudoun County	276,000
Knowink	James City County	61,000
Robis Elections	Montgomery	60,000
Knowink	Wise County	24,000

Requirements:

Participants will follow a similar set of regulations as outlined in 1VAC20-70-60 Security Requirement for Absentee Offices to conduct the pilot.[4] To participate in the pilot, localities must complete the following steps prior to Election Day:

- Localities must provide their Electronic Pollbook vendor with their approved network connections. The vendor will program the Mobile Device Manager (MDM) to allow the devices to access specific secured networks.
- Localities must comply with the Secure Connection Requirements, which may be referenced in the appendix.[5]

[4] 1VAC20-70-60 Security Requirements for Absentee Satellite Offices

[5] Satellite-Early-Voting Readiness-Checklist, https://www.elections.virginia.gov/media/formswarehouse/absentee-voting/Satellite-Early-Voting-Readiness-Checklist-FINAL-(1).pdf

- Localities must submit a list of all polling locations no less than 60 days before the election. The listing in the state voter registration system is submission.
- Eight days before the General Election, the locality will conduct a test to validate internet connectivity for all the precinct devices and submit confirmation of connectivity to the Department of Elections through Integra with an attestation letter in the Legal section signed by two locality officials responsible for testing the devices.
- Each polling location must have reliable internet connectivity for the entire day of the election. *Reliable* is defined by a connection that meets the National Institute of Standards and Technology standards and that the likelihood of connectivity interruptions is low.

Additionally, localities must also meet all MSS standards listed in the addendum of this document. Failure to comply with any of these requirements will result in exemption from the pilot.

Anticipated Challenges:

Cloud or VPN Drops: If the Cloud or VPM drops, EPB will continue to operate offline. As soon as a connection is re-established, the EPB will sync the data. Pursuant to §24.2-611F, a copy of a paper pollbook is required in case the electronic pollbook fails to operate properly.[6]

Voter Perception: Connection to the VPN or Cloud creates the perception that electronic pollbooks are more vulnerable to cyberattacks. For the past two-elections, ELECT has been allowing EPBs to connect to the VPN or Cloud at satellite voting sites without issue. The next step in this process is to test wireless connectivity in a limited capacity on Election Day. Easing into this process will build public confidence for a statewide plan to allow EPBs to connect to the VPN or Cloud on Election Day, while allowing ELECT to develop informed guidance and best practices for a smooth transition. ELECT will follow up with a report of the pilot and develop educational materials to inform the public and promote transparency of the process.

ANALYSIS

After the General Election, a report will be generated over the findings of the pilot and posted on ELECT's website. Additionally, localities selected for the pilot will be required to fill out a survey designed by ELECT staff and to attend one post-election meeting to evaluate the effectiveness of the study. General registrars participating in the process may be asked to review and provide feedback on any future guidance put forward by the Department regarding EPB connectivity on Election Day.

Addendum:

[6] §24.2-611 Form and Signing of pollbooks; records of persons voting; electronic pollbooks, https://law.lis.virginia.gov/vacode/24.2-611/

ADDENDUM - Secure Connection Requirements

The following controls must be met for VPN and or Wireless connection:

ACCESS CONTROL (Remote Access – Identification and Authentication)
Control Description:

Access is limited and restricted using the principle of "least privilege" and remote users are identified, authenticated and authorized. The wireless access points are encrypted and configured to generate security logs and monitor for issues and confirmed with documented technical security controls.

SYSTEMS COMMUNICATIONS – (Boundary Protection – Monitoring)
Control Description:

The information system is configured to monitor and control communications at the external boundary of the system and key internal boundaries within the system and external networks are managed and arranged with effective, security architecture.

Sensitive information and data is encrypted and boundary devices (e.g firewalls, routers) are configured to protect and control access to information resources. The locality (with IT Operations) employs monitoring tools to detect denial of service attacks and port protection are utilized to prevent connection to unauthorized equipment.

SECURITY INTEGRITY – (Monitoring - Audit Accountability)
Control Description:

The information systems are monitored and measures are implemented to detect information system unauthorized (local, network and remote) access. The systems are configured with real time malware/anti-virus/malicious code scanning. Audit records are kept for actions taken, who took the actions and time of the actions and configured to utilize Network Time Protocol (NTP) time synchronization. The audit records are protected from unauthorized account modification and detection and provides forensic results and reporting capabilities.

CONFIGURATION MANAGEMENT
Control Description:

System and architectural changes are analyzed for security ramifications and configuration change decisions are documented. Only qualified and authorized individuals are allowed access to initiate changes.