# Internet Voting

Brittany Westfall

West Virginia Secretary of State's Office

bwestfall@wvsos.com

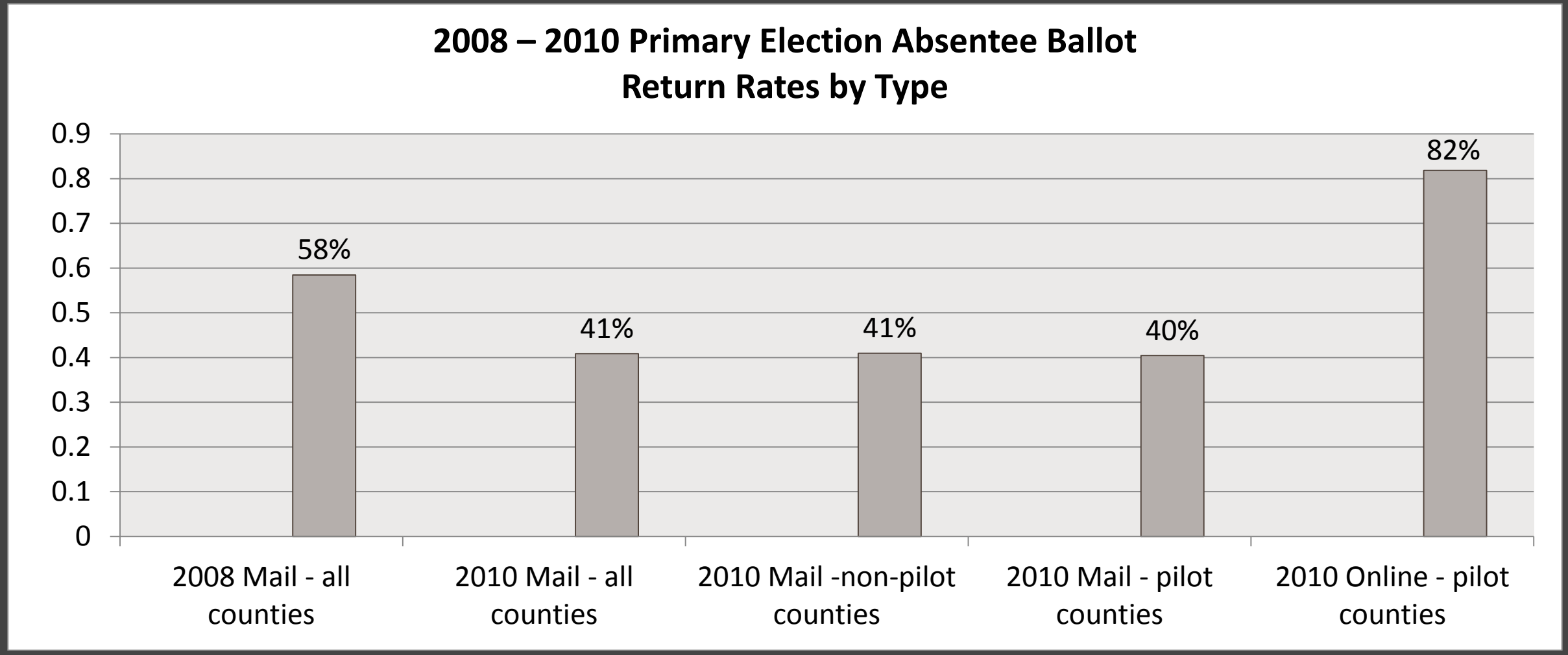
# WV 2010 UOCAVA Online Voting Pilot Project

- MOVE Act of 2009
- Five counties participated in the primary election and eight counties participated in the general election
- Two approved vendors partnered with the counties
- Due to outreach efforts, UOCAVA ballot requests increased
- Ballot return rate increased
- Voters who participated in online voting in the primary election also participated in the general election
- Primary election: 77 voters participated with a ballot return rate of 82%
- General election: 165 voters participated with a ballot return rate of 75.76%; this exceeds the 58% return rate using standard mail

# WV 2010 UOCAVA Online Voting Pilot Project

1. Voter applies for a ballot outside of the system
2. County provides voter email and ballot content to vendor
3. Vendor emails voter with a link to the website, along with a unique personal identifier
4. Voter enters personal identifier, along with additional personally-identifying information
5. Voter marks choices on screen
6. Voter may review choices then select “Cast Vote” link on the website; the voter’s choices are final
7. Voter receives a receipt code where he or she may later track the progress of the ballot

# WV 2010 UOCAVA Online Voting Pilot Project



# WV 2010 UOCAVA Online Voting Pilot Project

| General Election<br>Online Voting Participation Rates | | | | |
|---|---|---|---|---|
| **County** | **Applicants** | **Votes Cast** | **Vendor** | **% Votes Cast** |
| Jackson | 13 | 10 | Scytl | 76.92% |
| Kanawha | 41 | 35 | Everyone Counts | 85.37% |
| Marshall | 31 | 9 | Scytl | 29.03%* |
| Mason | 3 | 1 | Scytl | 33.33% |
| Monongalia | 22 | 22 | Everyone Counts | 100.00% |
| Monroe | 3 | 3 | Everyone Counts | 100.00% |
| Putnam | 16 | 15 | Everyone Counts | 93.75% |
| Wood | 36 | 30 | Everyone Counts | 83.33% |
| **TOTALS** | **165** | **125** | | **75.76%** |

# WV 2010 UOCAVA Online Voting Pilot Project

- Redundant servers
- 2048-bit encryption
- Secure Socket Layer (SSL)
- Ballot stored in encrypted format on the host server
- Non-networked computer for the decryption process
- Multiple key holders
- Ballots disassociated voter-identifying information
- Ballots are printed and entered in the same manner as other absentee ballots

From an overseas voter:

*"I will be working in the Kingdom of Saudi Arabia for at least the next two years. This program has enabled me to still cast my vote from 8500 miles away. I have nothing but praise for this system."*

From a military voter:

*"Thank you for allowing Monroe County as a Pilot Program in Voting Online. I am presently in Iraq on assignment with Operation Iraqi Freedom and this online voting process gave me a chance to Vote here while in a Combat Zone. Many of our soldiers last election did not have their vote counted due to being overseas in a combat zone. That was wrong for their vote Not to count. This way that you have developed is excellent. Thank You."*

# Security

Ballot Secrecy

- The secrecy of the ballot should not depend on a voter's device
- It prevents voter coercion and vote buying
- Is the secret ballot an opportunity or a requirement?

Independent Panel on Internet Voting, Recommendations Report to the Legislative Assembly of British Columbia, February 2014.

# Security

Ballot Secrecy and Confidentiality

- Internet voting may provide greater ballot secrecy than mail-in
  - Access control and cryptographic technologies
  - Allow voters to cast more than one ballot and only count final vote
- Recommendations:
  - Voter should not be linked to ballot
  - Encrypted storage of personal information and access control
  - No ballot receipt
  - Sensitive information, e.g., passwords and voter timestamps, should only be readable to authorized users
  - Should only store necessary information
  - Only necessary information should pass between voting system components (web, database, and application server)

National Institute of Standards and Technology Interagency Report: 7770, Security Considerations for Remote Electronic UOCAVA Voting, February 2011.

# Security

Threats to Ballot Secrecy and Confidentiality

- Data breaches
- Coercion
- Vote buying and selling
- Malicious software on voter's system

Current Solutions

- Cryptographic protection of data from the voter's system to the voting system: Secure Socket Layer (SSL) or Transport Layer Security (TSL)
- Downfalls: voter mistakes, malware, unreliable communication lines

National Institute of Standards and Technology Interagency Report: 7770, Security Considerations for Remote Electronic UOCAVA Voting, February 2011.

# Security

System Integrity

- Auditability
- Track events and trace activity
- Verification
- Testing and analysis
- Advanced end-to-end cryptography
- Malware detection/prevention

National Institute of Standards and Technology Interagency Report: 7770, Security Considerations for Remote Electronic UOCAVA Voting, February 2011.

# Availability and Accessibility

- Ballot Tracking
- Time Allowed for Voting and Reliability
- Recoverability, Fault-tolerance, Fail-Safe, and Scalability
- Compatibility with Accessibility Software and Hardware
- Usability
- Digital Divide

Independent Panel on Internet Voting, Recommendations Report to the Legislative Assembly of British Columbia, February 2014.

# Auditability

- Specialized skills and knowledge
- Built-in audit functions
- Third-party auditors
- Issue with providing a paper ballot count
- End-to-end verifiable (E2E) cryptographic systems
  - Was the ballot marked as intended?
  - Was the ballot collected by the system as the voter marked it?
  - Was the ballot counted as the voter cast it?

Independent Panel on Internet Voting, Recommendations Report to the Legislative Assembly of British Columbia, February 2014.

# Auditability

- Event logs and Reports
- Verifiability
- Ability to determine what entity created an election record
- Ability to verify that only authorized software is present on voting systems
- Mathematical proofs

National Institute of Standards and Technology Interagency Report: 7770, Security Considerations for Remote Electronic UOCAVA Voting, February 2011.

# Trust

- Threats to trust:
  - Lack of knowledge creates distrust
  - Voters trust election administrators to conduct fair elections; if an election is compromised during internet voting, the legitimacy of the government is at stake
  - Voters will not be able to observe the process
  - Election workers are replaced by IT experts
  - Fear of the “privatization of democracy”
- Build trust:
  - Publicize information about the internet voting system
  - Ensure proper testing
  - Develop mechanisms to certify and audit the system
  - Verify and evaluate

Independent Panel on Internet Voting, Recommendations Report to the Legislative Assembly of British Columbia, February 2014.

# United Kingdom

- Local governments piloted internet voting in 2002, 2003, and 2007
- 2002 - the UK Electoral Commission gave a positive report
- 2003 – UK Electoral Commission provided security recommendations
- 2007 – UK Electoral Commission find the pilots were successful, but show concerns:
  - Pre-registration contributed to lower use
  - Accessibility
  - Public understanding of the process
  - Technical problems in on jurisdiction
  - Lack of quality assurance and testing = risk
- The Commission recommends that no further internet voting pilots be conducted until a comprehensive strategy and standards for evaluation are set.

# Canada

- Ontario 2003: 12 municipalities (largest: Markham - 158,000)
- Ontario 2006: 20 municipalities (largest Markham)
- Nova Scotia 2008: 4 municipalities (largest: Halifax – 279,000)
- Ontario 2010: 44 municipalities (largest Markham)
- Nova Scotia 2012: 13 municipalities (largest Halifax)
- Edmonton 2012 (817,000) “Jelly Bean Election”

# Independent Panel on Internet Voting Recommendations

- Do not implement universal internet voting for either the local government of provincial government at this time; if it is implemented, it should be limited to individuals with disabilities; risks remain substantial
- Establish an independent technical committee to evaluate systems
- Evaluate systems based on principals established by the panel: accessibility, anonymity, verifiability, non-reliance on voter's device, one vote per voter, voter eligibility, service availability, authentication and authorization

Independent Panel on Internet Voting, Recommendations Report to the Legislative Assembly of British Columbia, February 2014.

# United States

- 2000 Pilot: South Carolina, Florida, Texas, Utah
- 2004 Secure Electronic Registration and Voting Experiment (SERVE) – cancelled
- 2010 Primary and General elections: WV Pilot Project
- September 2010: Washington D.C.’s internet voting test
- Although NIST encouraged pilot projects in the 2011 report, in May 2012, they proposed that additional research is needed before secure internet voting is feasible