THREATS TO VOTER REGISTRATION
Interaction of Voting and Election Systems

- Voting System
  - (re)Districting Systems
  - Auditing Systems
  - VR System
    - Online VR System
    - Auto VR System
  - Voter Information System
  - Ballot Tracking System
    - UOCAVA / Ballot Delivery/Return
    - Ballot Printing
      - Precinct Mgt Systems
    - Ballot on Demand
      - Voter Authentication System
      - Cap & Tab
        - Define Bal.
          - Reports
            - Audits
    - GIS
      - Candidate Qualifying System
      - E-pollbooks
        - Barcode Scanner
          - Statewide Election Night Reporting
            - Administrative Reports
              - Absentee Application

© 2017 Precinct Mgt Systems
Statewide Voter Registration Database

- Paper Poll Book
- Electronic Poll Book

Continual Updates

Self Registration
3rd Party Registration
Online Registration
DMV

Data Exchanges
Source of New Voter Registration Forms, 2016

Department of Motor Vehicles: 33%
Online: 17%
Mail, email, fax: 17%
Other: 15%
In person at local election office: 12%
States with Same Day and Election Day Registration

Legend:
- States that have enacted same day registration, including on election day.
- States that have allowed same day registration only during the early voting period.
- States that have passed election day registration but have not implemented it.
Automatic Voter Registration

DMV (or other designated agency)  Election Officials
Protecting Voter List Information

- Who can access voter lists?
- What information on voters is available to requestors? Does it include personal identifiable information?
- What information is contained in the statewide voter registration database? If a hack occurred, what information on voters could be accessed?
- Restrictions on use of the voter list
- Voter roll audit
The Tech Angle

• Which technologies are used?
• What are the potential security gaps?
• How could you disrupt registration?
Technologies Used

• Local IT infrastructure
  • Who owns & supports your IT system?

• Cloud-based infrastructure
  • Audit the security policies & procedures of vendors

• Web-based or App-based voter access
  • Remote authentication

• Communication encryption
  • TLS for web traffic

• Input Validation
  • Only allow limited character set in text field
Potential Security Gaps

• Phishing
• Network & Internet connectivity
• Security weaknesses in underlying commercial-of-the-shelf (COTS) products
• Errors in authentication & access control management configuration
• Data validation
• Backup & auditing
Disrupting Registration

• Fake registrations
• Misinformation
• Unauthorized access
• Targeting upstream state & cloud-based infrastructure
Group 1 Scenario:

Before Election Day you discover that a local election official has fallen prey to a spear phishing attack that has permitted nefarious actors access to the statewide voter registration database. It is unclear if any voter registration records have been changed. What can you do in the moment? Is there a legislative option to consider next session?
Group 2 Scenario:

The media is reporting that all of your state’s voter registration records, which include voters’ full addresses, driver’s license numbers and dates of birth, have been posted online. What can you do in the moment? Is there a legislative option to consider next session?
THREATS TO VOTING ITSELF
Where We Vote

Mail Voting

Vote Centers

Traditional Neighborhood Polling Places
Returning Ballots

- Absentee Ballots
- In-Person Locations
- Electronically Transmitted Ballots

Ballots Received by Local Election Official
Accommodating Voter Groups

• Voters with disabilities
• Rural voters
• Native American voters
The Tech Angle

• What are security procedures usually in place during the voting process?
• Where are the potential gaps?
Security Procedures

• Administrative controls
  • Defined & document roles, responsibilities, policies

• Technical controls
  • Defense in depth by design

• Physical controls
  • Locks, seals, surveillance, chain of custody, inventory
Potential Security Gaps

• Aging machines
  • Proper maintenance & replacement critical
• No paper trail
  • Voter verifiable paper trail required for audits
• Exploiting accessibility features
  • Accommodation adds complexities
• Information siloes
  • Channels of communication, security clearance
• Malware
  • Locks outs systems or destroys data
A Brief History of Voting Technology
A Brief History of Voting Technology
A Brief History of Voting Technology
### How States Plan to Use 2018 HAVA Funds

<table>
<thead>
<tr>
<th>Category</th>
<th>States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td>AL, IA, NE, SC, WY, AS, ID, NJ, SD, AZ, IL, NM, TN, CA, IN, NV, TX, CO, KY, NY, VI, CT, MA, OH, UT, DC, MD, OK, VA, FL, MI, OR, VT, GA, MN, PR, WA, HI, NC, RI, WI</td>
</tr>
<tr>
<td>Voting Equipment</td>
<td>AK, HI, NM, VT, AR, ID, OK, WV, AS, KY, PA, WY, CA, LA, RI, CO, MA, SC, CT, MD, SD, DC, MO, TN, DE, ND, TX, GA, NE, UT, GU, NJ, VA</td>
</tr>
<tr>
<td>Reserve</td>
<td>AS, MS, VA, CA, NE, VI, CO, NH, WA</td>
</tr>
<tr>
<td>Voter Registration</td>
<td>AL, ID, NV, CA, NE, WA, VA</td>
</tr>
<tr>
<td>Election Audits</td>
<td>AL, MI, VA, CA, MN, VT, CO, NC, WA, CT, NJ</td>
</tr>
<tr>
<td>Communication</td>
<td>AS, MI, CO, NE, CT, NJ, DC, NV, FL, VA, GU, VI, IA, WV, ID, IN, MD</td>
</tr>
</tbody>
</table>
Post-Election Audits
Post-Election Audits: Things Legislators Could Address

- Require post-election audits
- Voting equipment with a paper trail
- The audit scope – what is audited and what percentage?
- Consider a risk limiting audit
- When is the audit conducted
- What happens if there is a discrepancy?
Use of the Internet to Facilitate Voting

- Blank ballot delivery
- Electronically transmitted ballots from some
- Remote ballot marking tools
- Voter information and polling place lookup
- Publish unofficial results
The Tech Angle

• Which technologies are used?
• What security issues could there be with using the Internet to facilitate voting?
Technologies Used

• Two-factor authentication
  • Passwords, tokens, biometrics
• Social media
  • Outreach on multiple platforms
• Blockchain
  • Internet connection, all encryption eventually broken
• Local IT infrastructure
• Cloud-based infrastructure
• Web-based or App-based voter access
• Communication encryption
• Input Validation
Potential Security Issues

• Spoofing identity of voters
  • Limited set of authorized voters & election officials

• Outdated encryption
  • Use httpS

• Misinformation
  • Use Election Buster to check for imposter accounts
Group 1 Scenario:

Three months before the election, a news report indicated that some of your optical scan vote counting equipment has the ability for the vendor you bought it from to “remote access” the software. This is intended to allow fixes without a service call to the site. And yet, security advocates say having that ability causes a vulnerability for hackers. What can you do in the moment? Is there a legislative option to consider next session?
Group 2 Scenario:

On Election Day, an unusual number of people have arrived to vote, only to find that their names are not on the electronic poll book in that precinct. It is possible they are in the wrong polling place, or that an error was made. Is it possible to help them vote? What might be the problem? Is there a legislative option to consider next session?
THREATS TO REPORTING RESULTS
The Tech Angle

• Which technologies are used?
• What are the potential security gaps?
• How could you disrupt an election?
Technologies Used

• Scalable infrastructure
  • Buying additional capacity as needed
• Albert network sensors
  • Share actionable information with other jurisdictions
• Social media
  • Set expectations for update intervals & sources
Potential Security Gaps

• Dedicated devices
• Polling place support
• Network & Internet connectivity
• Security weaknesses in underlying commercial-of-the-shelf (COTS) products
• Errors in authentication & access control management configuration
• Data validation
Disrupting Reporting Results

• Denial of service attacks
  • Free services to protect against automated attacks
• Misinformation
  • Prepare a communication plan
Scenario

After the polls have closed, the election night reporting website, where unofficial results are posted for the media and the public (and where tallies from local jurisdictions come together), goes down. There is a closely watched Senate race so the national media are anxious for results. How can this event be handled in the moment? Is there a legislative option to consider next session?
2018 MIDTERMS RECAP
Questions?

Katy Owens Hubler
435-647-6051
katy@democracyresearch.com

Maurice Turner
202-224-8819
Maurice@cdt.org
@TypeMRT