5 September, 2016

Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections

Recent high-profile cyber-attacks have drawn public attention to the security of U.S. election systems. Keeping election systems reliable and safe is an evolving challenge, as it is for any computer system. Security experts recommend the following for all computer systems, from laptops to mainframe software:

- Secure systems as well as possible and make security updates regularly.
- Assume that an attacker will breach even the best security.
- Be vigilant for signs of a breach.
- Prepare contingency plans.

Election systems have additional requirements for transparency and accuracy so the public can have confidence in election outcomes.

As computer security expert Bruce Schneier has noted, "We tend to underestimate threats that haven't happened – we discount them as theoretical…. Russian attacks against our voting system have happened. And they will happen again, unless we take action."

The ten recommendations below address these concerns by providing specific steps election officials and individuals can take during the next few weeks to reduce risk and improve public confidence in the upcoming elections. Because of local laws and regulations, not every suggestion will be appropriate to every election jurisdiction.

Many state and local election officials have already taken a number of the steps outlined below, and other groups have suggested similar actions that can be taken to increase election integrity and public confidence. But much still remains to be done.

The following list is limited to actions that can be taken in the next few weeks preceding and immediately following the election. We look forward to working with election officials and others on longer-term improvements that will increase public confidence in future elections.

Members of the Election Verification Network compiled this list in response to a recent invitation from Election Assistance Commission (EAC) Chairman Thomas Hicks. For further information, please contact the Election Verification Network.

Editors (with affiliations for identification purposes only):
John McCarthy, Verified Voting Foundation
Stephanie Singer, former Chair of the Philadelphia County Board of Election
Lawrence Norden, Democracy Program, Brennan Center for Justice at NYU School of Law
Whitney Quesenbery, Center for Civic Design
Mark Lindeman, Professor of Political Science, Bard College
Andrew Appel, Professor of Computer Science, Princeton University
Kim Alexander, President and Founder, California Voter Foundation
Joe Kiniry, Galois and Free & Fair

1. Document and review security fundamentals

- List all equipment, including USB drives and memory cards. Note when each piece of equipment might be connected to the Internet (even briefly), and which systems have wireless capabilities.
- Manage access controls. For each system, list everyone who can access the system, including elections staff and third-party vendor staff. Require strong passwords for all users.
- Ensure background checks are completed for both permanent and temporary staff with access to sensitive systems, and disable access when staff leave the organization.
- Limit physical access and regularly audit sensitive and critical election systems.
- Ensure that all PC and server operating systems and software have the latest security patches.
- Train all staff on fundamental security practices.

2. Test all election systems for security vulnerabilities and ability to detect attacks

- Include voter registration, ballot delivery, voting machines and election management systems.
- Document and update pre-election testing protocols and conduct pre-election testing.
- Review and document compliance with the recommendations and security checklists prepared by the US Department of Homeland Security on best practices for security, penetration testing, network scanning, how to detect and deal with potential cyber-attacks, etc.
- Review and track FBI security alerts, such as the alert "Targeting Activity Against State Board of Election Systems" recently reported in Yahoo News.
- Identify resources employed to review and assess security protocols. Where feasible, ask for third-party review of those protocols (for example, county and state IT staff with security expertise).
- Excellent resources for robust pre-election testing can be found at Washburn Research.
- Contact the Election Verification Network to find credentialed volunteer experts.

3. Reduce risks created through voting systems' connections to the internet

- For those states allowing transmission of voted ballots over networks outside the control of election officials, each voter should be warned on the website and as part of the voting process: "Returning ballots by Internet, fax or email should only be used as a last resort. Voting in person or with a mailed in absentee ballot is more secure and preserves the secrecy of the ballot."
- Assume that ballots submitted over the Internet contain malware. Print them out for official tally and retention. Carefully document and authenticate any ballots returned over the Internet.
- Document and review protocols in place for confirming and verifying online registration transactions, especially changes to registrations.
- Remind staff how to detect and report unusual system malfunctions and abnormal audit results.

4. Plan for electricity, telephone, computer or communications disruptions

- For each system, detail contingency procedures (in writing) in case of failure of electricity, telephone, computer or communications systems for both voting places and central facilities.
- Create paper backups for all electronic systems such as poll books, electronic ballots, etc. and create contingency distribution plans for these paper backups.
- Develop and distribute written plans for contingencies; what will you do if
  - Your voter registration database becomes corrupted?
  - Pollbooks in some locations appear to be corrupted?
  - Too many voters require provisional ballots?
  - Wait times for voting become excessive in certain locations?
  - Many electronic voting systems refuse to turn on?

5. Train election staff and poll workers how to detect and respond to problems.

- See specific recommendations for Election Day checklists, security, etc. in "Security insights and issues for poll workers" from the Center for Civic Design.
- Create and promote a forum (such as a Facebook page) for poll workers to ask and answer questions about procedures.
- Review and update documentation about how to handle challenging and unexpected situations at the polls: long lines, unauthorized observers, equipment failures, inaccurate poll books, etc.

6. Provide clear guidance on reporting election security issues and other problems

- Create an online form and a toll-free hot-line number for reporting election security issues or other problems, or add this feature to existing reporting systems. Monitor online forms and hotlines frequently before, during, and after the election.
- Encourage everyone to report suspicious behavior by anyone with access to the election systems.
- Contact state agencies, Election Assistance Commission, and Department of Homeland Security to plan real-time reporting to these agencies in case of unfamiliar voting system problems.
- Provide opportunities for anonymous reporting and protection from retaliation.

7. Encourage public participation and observation of all election procedures allowed by law

- Post information prominently on your website and send press releases to local reporters, community groups and political parties inviting the public to observe.
- Publicize dates, times and locations of procedures beyond what is required by law.
- Publicize a calendar of steps leading to the election (with locations if open to the public): deadlines for voter registration and absentee, military, and overseas ballot applications; ballot

design and printing deadlines; pre-election testing; election training sessions; poll opening and closing; precinct and central vote counting, and all canvassing and auditing dates and sites.

- On your web site, post copies of manuals for all procedures the public is permitted to observe, and post descriptions of procedures that the public is not permitted to observe.
- Publicize the procedures for citizens or citizens' groups to obtain permission to access records, observe procedures and verify integrity.
- For each kind of ballot (such as absentee, early voting, in-precinct, provisional), document the chain of custody of the ballot from the time the blank ballot leaves the central office to the time the voted ballot is canvassed.

8. Conduct post-election audits before certification of final results

- Without voter-verified paper ballots, effective audits are impossible.
- Compare statistical samples of voting system totals to hand counts of matched paper ballot sets.
- Recruit technical experts to assist with tests and audits. Resources for finding experts, many of whom may provide pro bono services, include the Election Verification Network, professional societies such as the American Statistical Association, and academic institutions.
- Prominently publicize all testing and audit results.

9. Report and publicize ballot accounting and final results in detail before certification

- Create ballot accounting reports by jurisdiction, broken down by vote location (including vote centers) and ballot type (regular, provisional, absentee, etc.).
- Include the total number of ballots cast, not just results of contests.
- Reconcile number of ballots created, number voted and number returned with counts of voters.
- If counting procedures mingle ballots from different categories (for example, if ballots cast at a vote center are mingled with precinct election-day ballots), create and distribute an explanatory document to help outside observers verify that the numbers make sense.

10. Document problems and note procedures that will require additional resources to implement

- Work with the EAC and other election jurisdictions to suggest areas for future improvement.
- Note what worked well and what needs improvement to help write best practices for the future.
- Contact the Election Verification Network if you would like to work with other election experts on improving future elections.