Committee on House Oversight and Government Reform,
Subcommittee on Information Technology
United States House of Representatives

Statement of Lawrence D. Norden
Deputy Director, Democracy Program,
Brennan Center for Justice at NYU School of Law

September 28, 2016

"Cybersecurity: Ensuring the Integrity of the Ballot Box"

On behalf of the Brennan Center for Justice, I thank the Subcommittee on Information and Technology for holding this hearing. We appreciate the opportunity to share with you the results of our extensive studies to ensure our nation's voting systems are more secure and reliable. The Brennan Center for Justice is a nonpartisan think tank and advocacy organization that focuses on democracy and justice. We are deeply involved in the effort to ensure accurate and fair voting, improve voter registration, and to promote policies that maximize participation of eligible citizens in elections.

For the last decade, I have led the Brennan Center's extensive work on voting technology and security. In 2005, in response to growing public concern over the security of new electronic voting systems, I chaired a task force (the "Security Task Force") of the nation's leading technologists, election experts, and security professionals assembled by the Brennan Center to analyze the security and reliability of the nation's electronic voting machines.[1] In the decade since, I have authored or co-authored numerous studies on election system security, usability, cost and design.[2] Most recently, with my colleague Chris Famighetti, I co-authored *America's Voting Machines at Risk*, a nearly year-long study that combined data from various public documents with surveys of more than 100 specialists familiar with voting technology, including voting machine vendors, independent technology experts and election officials in all 50 states.[3] The report details the security and reliability risks associated with continuing to use equipment around the country that is rapidly approaching the end of its projected lifespan.

[1] LAWRENCE NORDEN, BRENNAN CTR. FOR JUSTICE, THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY, AND COST 46 (2006), *available at* https://www.brennancenter.org/sites/default/files/publications/Machinery_Democracy.pdf.

[2] *See e.g*. LAWRENCE NORDEN ET AL., BRENNAN CTR. FOR JUSTICE, POST-ELECTION AUDITS: RESTORING TRUST IN ELECTIONS (2007), *available at* http://www.brennancenter.org/sites/default/files/legacy/d/download_file_50227.pdf.; LAWRENCE NORDEN, BRENNAN CTR. FOR JUSTICE, VOTING SYSTEM FAILURES: A DATABASE SOLUTION (2010), *available at* http://www.brennancenter.org/sites/default/files/legacy/Democracy/Voting_Machine_Failures_Online.pdf.; LAWRENCE NORDEN ET AL., BRENNAN CTR. FOR JUSTICE, BETTER BALLOTS (2008), *available at* http://www.brennancenter.org/sites/default/files/legacy/Democracy/Better%20Ballots.pdf.; LAWRENCE NORDEN ET AL., BRENNAN CTR. FOR JUSTICE, BETTER DESIGN, BETTER ELECTIONS (2012), *available at* http://www.brennancenter.org/sites/default/files/legacy/Democracy/VRE/Better_Design_Better_Elections.pdf.

[3] LAWRENCE NORDEN & CHRISTOPHER FAMIGHETTI, BRENNAN CTR. FOR JUSTICE, AMERICA'S VOTING MACHINES AT RISK 4 (2015), *available at* https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

Recent high profile hacks, particularly those related to the election, have raised public fears about the integrity of our voting system. I hope to convey four points in my testimony today:

A. Any attempt to interfere with the integrity of American elections must be treated with extreme seriousness. Among other things, this means that **it is essential to distinguish between genuine threats from sensationalistic and heated rhetoric**;

B. The **biggest threats to the integrity** of this November's election and our democratic system are **attempts to undermine public confidence** in the reliability of that system. Attacks against the voting machines upon which Americans cast their ballots are highly unlikely to have a widespread impact. By contrast, attacks or malfunctions that can undermine public confidence are much easier;

C. There are **important steps that election officials and the public have taken and should take to secure this November's election** against attack or malfunctions that could impact election outcomes or public confidence in those outcomes;

D. Longer term, we must invest in our nation's election technology infrastructure and **replace the oldest machines and equipment that over time will become less reliable and less secure.** An election with integrity will ensure that all eligible citizens have the opportunity and ability to vote, and have confidence that their votes will be counted.

I. Distinguishing genuine threats from sensationalistic rhetoric

To address and combat potential threats to the integrity of our elections, we must honestly assess the risks and distinguish between what is probable, possible, and conceivable but highly unlikely. In recent weeks, various sources in the media and elsewhere have raised fears of widespread hacking and fraud that could change the outcome of this November's national election. These fears are generally supported by speculation and partial information.

This is harmful to our democracy, which critically depends on the confidence of the people. Hyperbolic or inaccurate rhetoric undermines the hard work election officials are doing to ensure our elections run smoothly and shifts attention away from addressing the very real problems our election system faces.

It can be especially harmful in the event of a close national election. As I will discuss below, any attempt to attack our voting systems is far more likely to sow doubt about results than it is to change a large numbers of votes. At the same time, as equipment ages, malfunctions—such as calibration problems on touch screen machines, or freezes that result in machines being taken out of service —can become more common and further compound this mistrust.[4]

[4] NORDEN & FAMIGHETTI, *supra* note 3, at 12-14.

II. Assessing the relative risks of attacks against our election system, and steps to secure them.

When voters hear of "hacks" against our election systems, many are unlikely to distinguish between campaign e-mail servers, voter registration databases and the voting machines on which they cast their votes. Not surprisingly, after hacks against the DNC e-mail server and state registration databases were revealed, many media reports immediately jumped to the question of whether our voting machines could be hacked.[5]

For this reason, it is critical to distinguish between campaign email servers and registration databases, which are connected to the internet, and voting machines, which should never be connected to the internet. For obvious reasons, it is far easier to attack a system remotely if it is connected to the internet than if it is not.[6]

A. Threats to Voter Registration Systems and Steps to Protect Them

In the last month, we learned of attempted intrusions into the Illinois and Arizona voter registration databases. It appears that in Arizona, the state detected the attempted hack before records could be accessed.[7] In Illinois, hackers accessed personal data from several thousand voter records, but it does not appear that any voter data was changed and the full voter registration list remained unaffected.[8]

There are evident reasons to be concerned about hackers accessing voter registration databases. The first is related to accessing of personal information. Depending on how that personal information is stored, by successfully accessing a state's registration database, hackers may be able to obtain enough information to use it for identity theft. For this reason alone, it is critical that election officials run frequent scans to monitor and alert them for potentially abnormal activity, and otherwise employ best practices to protect against hacking. The Election Assistance Commission has provided useful guidance for securing voter registration data.[9] Both the FBI and DHS have expertise in this area, and my understanding from several election officials around

[5] *See* NPR Staff, *After DNC Hack Cybersecurity Experts Worry About Old Machines, Vote Tampering,* NPR, Aug. 20, 2016, http://www.npr.org/sections/alltechconsidered/2016/08/20/490544887/after-dnc-hack-cybersecurity-experts-worry-about-old-machines-vote-tampering.; Laurie Segall, *Just How Secure Are Electronic Voting Machines?* CNN, Aug. 9, 2016, http://money.cnn.com/2016/08/09/technology/voting-machine-hack-election/.; Brian Barrett, *America's Electronic Voting Machines Are Scarily Easy Targets,* WIRED, Aug. 2, 2016, https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/.

[6] *See* VA. INFO. TECHNOLOGIES AGENCY, SECURITY ASSESSMENT OF WINVOTE VOTING EQUIPMENT FOR DEPARTMENT OF ELECTIONS SECURITY ASSESSMENT (2015). *available at* http://www.elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf.

[7] Ellen Nakashima, *Russian Hackers Targeted Arizona Election System,* THE WASH. POST, Aug. 29, 2016, https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html.

[8] Tina Sfondeles, *Hackers Accessed Personal Info from 200,000 Illinois Voters*, CHI. SUN TIMES, Aug. 29, 2016, http://chicago.suntimes.com/politics/hackers-accessed-personal-info-from-200000-illinois-voters/.

[9] U.S. ELECTIONS ASSISTANCE COMMISSION, CHECKLIST FOR SECURING VOTER REGISTRATION DATA, *available at* http://www.eac.gov/assets/1/Documents/Checklist_Securing_VR_Data_FINAL_5.19.16.pdf.

the country is that they are working closely with both departments to ensure they are doing all they can to prevent future attacks.

A second reason for concern about hacking of voter registration databases is related to the integrity of the election itself. If a hacker were able to delete or change voter information, this could conceivably prevent someone from voting or having their vote counted, depending on the voting rules in the affected jurisdiction. The good news is that there are relatively straightforward steps that election officials can take to ensure that such attacks are thwarted or do not impact the ability of registered voters to vote.

Perhaps most importantly, election officials should create regular backups, including paper copies, of their registration databases. As long as this is done, no manipulation of computer registration databases should prevent legitimate voters from casting a ballot, or having their votes counted. Backup lists can be reconstructed and ensure that no voter is prevented from casting a ballot on Election Day.[10]

Voters can also help thwart attacks against voter registration databases. They should be encouraged to check their registration on-line before the registration deadline in their state, and before going to vote, and to inform election officials if their information has been changed or deleted.

B. Threats to Voting Machines

There are over 10,000 election jurisdictions in the United States.[11] This means in a federal election, there are essentially more than 10,000 separate elections being run, with different voting machines, ballots, rules and security measures. While there are security benefits and weaknesses associated with such a decentralized system, one clear benefit is that it is not possible to attack the nation's voting machines in one location, as might be possible with a statewide voter registration database or campaign e-mail server.[12] Similarly, because voting is not done on machines connected to the internet, remotely attacking these machines becomes difficult if not impossible.

Still, as I will discuss below, there is much more we should do to promote the security and accuracy of our voting systems. Computer scientists have demonstrated that older equipment, in particular, can be very insecure.[13] It is also more difficult to maintain, and more likely to fail

[10] For more detail on steps that jurisdictions can take to protect their registration databases *see* Appendix A, *Voting System Security and Reliability Risks*.

[11] *Election Administration and Voting Survey FAQs*, ELECTION ASSISTANCE COMMISSION, *available at* http://www.eac.gov/research/election_administration_and_voting_survey_faqs.aspx.

[12] *See* Dr. Dan S. Wallach, Testimony Before the House Committee on Space, Science & Technology Hearing 4, Sept. 13, 2016, at https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY-WState-DWallach-20160913.pdf

[13] Ben Wofford, *How to Hack an Election in 7 Minutes*, POLITICO (Aug. 5, 2016), http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144.; ARIEL J. FELDMAN ET AL., CTR. FOR INFO. TECH. POLICY AND DEP'T OF COMPUTER SCIENCE, PRINCETON UNIV., SECURITY ANALYSIS OF THE DIEBOLD ACCUVOTE-TS VOTING MACHINE (2006), *available at* https://www.usenix.org/legacy/event/evt07/tech/full_papers/feldman/feldman.pdf.; DAVID WAGNER ET AL., UNIV. OF

(even without interference from an attacker) on Election Day.[14] While small-scale attacks or failures of individual machines might not have a widespread impact on national vote totals, they can severely damage voter confidence, and would be particularly troubling in very close contests.

In the short run, we should do everything we can to minimize the impact of such attacks or failures.[15] In the long run, we must treat our election infrastructure with the importance it deserves, with regular investments and upgrades.

1. Recent Improvements to Voting Machine Security

Before detailing how election security and reliability can be improved, it is important to understand the significant steps taken over the last several years to protect the integrity of our elections.

While recent hacks deserve our attention, the overwhelming majority of voting is not done over the internet. In recent years, voting machines that had their own wireless networks and could be accessed remotely have been taken out of service, making remote attacks much more difficult.[16]

Just as importantly, since the Help America Vote Act was passed in 2002, the Election Assistance Commission developed standards for federal certification of voting systems, which were passed in 2005, and updated in 2015.[17] Today, 47 of 50 states rely on the Election Assistance Commission's (EAC) federal certification process when purchasing voting machines.[18] This process includes much more rigorous security testing than previously existed.[19]

Finally, in the last few years, many jurisdictions have replaced their paperless computerized voting machines with systems that scan paper ballots filled out by voters, or produce a paper trail that can be reviewed by the voter. The Brennan Center estimates that this November, at least 80 percent of registered voters will make selections on a paper ballot, or vote on an electronic

CAL., BERKELEY, SECURITY ANALYSIS OF THE DIEBOLD ACCUBASIC INTERPRETER (2006), *available at* http://nob.cs.ucdavis.edu/bishop/notes/2006-inter/2006-inter.pdf.

[14] NORDEN & FAMIGHETTI, *supra* note 3.

[15] *Election 2016 Controversies: Voting System Security and Reliability Risks*, BRENNAN CTR. FOR JUSTICE, https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf.

[16] Jenna Portnoy, *Va. Bd. of Elections Votes to Decertify Some Voting Machine,* THE WASH. POST, Apr. 14, 2015, https://www.washingtonpost.com/local/virginia-politics/va-board-of-elections-votes-to-decertify-some-voting-machines/2015/04/14/46bce444-e2a6-11e4-81ea-0649268f729e_story.html.

[17] BRYAN WHITENER, U.S. ELECTIONS ASSISTANCE COMMISSION, EAC UPDATES FEDERAL VOTING SYSTEM GUIDELINES, Mar. 31, 2015, *available at* http://www.eac.gov/assets/1/Documents/EAC%20Updates%20Federal%20Voting%20System%20Guidelines-News-Release-FINAL-3-31-15-website.pdf.

[18] *See* Charles H. Romine, Ph.D, Testimony Before the United States House of Representatives Committee on Science, Space and Technology, Sept. 13, 2016, at http://democrats.science.house.gov/sites/democrats.science.house.gov/files/documents/Romine%20Testimony.pdf.; BRIAN HANCOCK ET AL. BOWEN CTR. FOR PUBLIC AFFAIRS, INFRASTRUCTURE REQUIREMENTS FOR THE TESTING AND CERTIFICATION OF ELECTION SYSTEMS (2015), *available at* http://bowencenterforpublicaffairs.org/wp-content/uploads/2015/05/Infrastructure-Requirements-for-the-Testing-and-Certification-of-Election-Systems_FINAL.5.13.15.pdf.

[19] ROMINE, *supra* note 18.

machine that produces a paper trail.[20] This extra “software independent” record provides another important security redundancy that should act as a deterrent to attack, and should provide voters with more confidence that their votes have been counted accurately. A public post-election audit of the voting machines can be used to confirm that the electronic record reported by the machine is correct.

All systems that include a software independent record that can be reviewed by the voter and checked against the electronic total should be fully accessible to all voters with disabilities. The good news is that there has been significant progress to make sure this is possible in new voting systems.[21]

2. Outdated Voting Machines Pose Integrity Risks

Despite these advances, there is still more work to do to ensure that all voting machines are as secure and reliable as possible. In our 2015 report, *America’s Voting Machines at Risk*, the Brennan Center found that this November, 42 states will use voting machines that are at least 10 years old.[22] This is perilously close to the end of most machines’ projected lifespan, particularly machines designed and engineered in the late 1990s and early 2000s. Such machines make up the bulk of system purchased in the years following the passage of the Help America Vote Act. Using aging voting equipment increases the risk of failures and crashes — which can lead to long lines and lost votes.

The vast majority of paperless computerized voting machines were purchased at least a decade ago.[23] In November, some voters in 14 states will vote on these paperless machines.[24] Such machines do not produce record that can be reviewed by the voter, and allow election officials and the public to confirm electronic vote totals with a record that was produced independently of the software.

Aging voting systems also use outdated hardware and software. For this reason, replacement parts for older voting systems can be difficult, if not impossible, to find. Election officials reported to us that they struggle to find replacement parts for these systems (many of which are no longer manufactured) to keep them running. In several cases, officials have had to turn to eBay to find critical components like dot-matrix printer ribbons, decades old memory storage

[20] *See The Verifier—Polling Place Equipment—Current*, VERIFIED VOTER, https://www.verifiedvoting.org/verifier/.
[21] *Remote Ballot Marking Systems: Secure and Accessible*, CTR. FOR CIVIC DESIGN, http://civicdesign.org/projects/remote-ballot-marking/.; The Design Concepts, VOTING SYSTEMS ASSESSMENT PROJECT, http://vsap.lavote.net/design-concepts-2/.
[22] NORDEN & FAMIGHETTI, *supra* note 3, at 9.
[23] In the last few years we have seen a shift away from paperless machines to PCOS systems Abby Goodnough & Christopher Drew, *Florida to Shift Voting System With Paper Trail*, N.Y. TIMES, Feb. 2, 2007, http://www.nytimes.com/2007/02/02/us/02voting.html?_r=1.; *California Bans E-voting for Two Million in Four Counties*, USA TODAY NETWORK, May 1, 2004, http://usatoday30.usatoday.com/news/politicselections/2004-05-01-e-voting_x.htm.
[24] Delaware, Georgia, Louisiana, New Jersey and South Carolina use paperless electronic voting machines as their primary polling place equipment statewide. In Arkansans, Indiana, Kansas, Kentucky, Mississippi, Pennsylvania, Tennessee, Texas, and Virginia, some portion of polling places use such paperless machines as the primary equipment.*See* The Verifier—Polling Place Equipment—Current, VERIFIED VOTER, https://www.verifiedvoting.org/verifier/.

devices, and analog modems.[25] Aging systems also frequently rely on unsupported software, like Windows XP and 2000, which does not receive regular security patches and is more vulnerable to the latest methods of cyberattack.[26]

Finally, while nearly all of today's new voting machines go through a federal certification and testing program, many jurisdictions purchased voting machines before this process was in place. Older machines can have serious security flaws, including hacking vulnerabilities, which would be unacceptable by today's standards.

3. Steps Before November to Increase Security and Public Confidence

Americans should be comforted by the fact that while most of the public discussion of cybersecurity risks to our voting systems has happened only in the last few months, security experts and election officials have been in dialogue about this subject for years.[27] Long before there were stories in the media about Russian hacks into campaign e-mail servers or registration databases, these officials were working with federal, state and local officials to do everything possible to ensure our systems are secure and reliable. I know from personal conversations with election officials that many are in regular contact with the Department of Homeland Security, Federal Bureau of Investigation and the Election Assistance Commission about what they can do to redouble their efforts to ahead of November's election to help secure and inspire confidence in this year's election.

This year, working with election officials and others I have co-authored or edited *Voting System Security and Reliability Risks*, *Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections*, and *Guidance for Election Officials with Aging Voting Equipment.*[28] The key steps recommended in these documents are already being taken by many election officials, including:

- Documenting and reviewing security fundamentals, including physical security and chain of custody practices;

[25] Telephone Interview with Mark Earley, Voting Sys. Manager, Leon Cnty., Fla. (Jan. 26, 2015); Telephone Interview with Paul Ziriax, Secretary, Okla. Board of Elections, and Pam Slater, Assistant Secretary, Okla. Board of Elections (Mar. 16, 2015); Telephone Interview with Kristin Mavromatis, Public Information Manager, Mecklenburg Cnty., N.C. (Apr. 9, 2015).

[26] Telephone Interview with Merle King, Exec. Dir., Ctr. for Election Sys., Kennesaw State Univ. (Feb. 5, 2015); Telephone Interview with Joe Rozell, Dir. of Elections, Oakland Cnty., Mich. (Feb. 24, 2015); Telephone Interview with Neal Kelley, Registrar of Voting, Orange Cnty., Cal. (Feb. 2, 2015); Telephone Interview with Ryan Macias, Voting Sys. Analyst, Sec. of State's Office, Cal. (Mar. 13, 2015); Telephone Interview with Joseph Mansky, Elections Manager, Ramsey Cnty., Minn. (Apr. 30, 2015); Telephone Interview with Sherry Poland, Dir. of Elections, Hamilton Cnty., Ohio (Feb. 18, 2015); Telephone Interview with Garth Fell, Elections and Recording Manager, Snohomish Cnty., Wash. (Apr. 30, 2015); E-mail from Jeremy Epstein, Senior Computer Scientist, SRI Int'l, to Lawrence Norden, Deputy Dir., Democracy Program, Brennan Ctr. for Justice (May 30, 2015, 15:21 EST) (on file with author).

[27] NORDEN, *supra* note 1, at 46.

[28] *See* Appendix A for *Voting System Security and Reliability Risks*, *Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections*, and *Guidance for Election Officials with Aging Voting Equipment*

- Testing all election systems for security vulnerabilities and ability to detect attacks, including through robust public pre-election testing of every voting machine;
- Training election staff and poll workers how to detect and respond to problems, including long lines, unauthorized observers, equipment failures and inaccurate poll books.
- Ensuring sufficient emergency paper ballots are available at all places where Direct Recording Electronic voting machines are used.
- Conducting post-election audits to confirm that paper records match electronic results.
- Reviewing, and where necessary, improving "reconciliation policies" to guarantee that the number of signed-in voters matches ballot totals, and that machine and polling place totals match county and state totals.

Finally, voters can help secure our system as well. As with protecting the integrity of our voter registration lists (where voters have a vital role to play by checking their information and reporting any problems), voters can help ensure that any voting machine problems do not impact their or others' ability to vote. Among other things, voters should vote early when possible to avoid potential delays caused by machine breakdowns on Election Day. And if voters experience problems while voting on machines, or if those machines fail, they should immediately report those problems to local election officials or poll workers and then call 866-OUR-VOTE, the Election Protection hotline, to report the problem.

4. Long Term Solutions: State and Federal Action for Improving Security and Reliability

Ultimately, securing our elections and inspiring confidence in the long term requires further investment in our election infrastructure. While the need for more up-to-date, accessible, secure and reliable voting equipment is clear, funders at the state and federal level seem unconcerned about our aging voting infrastructure. In our interviews for *Voting Machines at Risk*, election officials in 31 states told us they would like to purchase and deploy new voting machines before the next presidential election in 2020. However, officials from 22 of those states said they do not know where they will get the money to pay for new machines.[29] More recently, we surveyed over 250 local election officials about their need to replace aging equipment. While a clear majority said they hoped to replace their equipment before 2020, approximately 80% of them said they did not have the money or a plan to do so.[30]

In too many states, legislatures have passed the buck to counties and towns. The frequent result, not surprisingly, is that counties with more resources and higher median incomes have replaced or have plans to replace antiquated equipment, while those with less resources, particularly poor or rural counties, are more left to cope with equipment that should be replaced.[31]

There are several steps we believe policymakers can take to ensure that our voting systems inspire confidence and are more secure and reliable over time:

[29] NORDEN & FAMIGHETTI, *supra* note 3, at 19.
[30] Forthcoming study from the BRENNAN CTR. FOR JUSTICE
[31] NORDEN & FAMIGHETTI, *supra* note 3, at 19.

- **Replace older equipment, particularly paperless direct recording electronic machines.**

    - Congress and state legislatures need to allocate the funds for new, reliable, and secure voting systems.
    - Machines purchased with these funds should be *auditable* in accordance with the definition and requirements set by the Auditability Working Group convened by the National Institute of Standards and Technology (NIST) and reported to the U.S. Election Assistance Commission. Specifically, *"[t]he transparency of a voting system with regards to the ability to verify that it has operated correctly in an election, and to identify the cause if it has not*."
    - The Auditability Working Group found that in order to satisfy these criteria a voting system must possess "Software Independence" or provide that an undetected change in the software cannot cause an undetectable error or change in the election outcome.[32]

- **Require audits of election results, using paper ballots or voter verifiable paper records, to confirm electronic totals.** Today, only 26 states require that election officials conduct paper audits.[33] Audits of paper records are an additional check on machine malfunction, and provide public verification of vote totals.

- **Create standards for Internet Voting**
    - Currently 31 states allow military and overseas voters to cast ballots by fax, e-mail or internet portal. Alaska allows any qualified voter to request and return an absentee ballot via facsimile.[34]
    - Most security experts argue that internet voting presents an especially serious security risk.[35]
    - There are currently no federal standards for voting over the internet, via fax or by e-mail. Given all that's come out about Russian involvement in hacking to influence the 2016 election, requiring new federal standards for such voting seems very important.[36]

- **Provide grants to fund voting technology improvements to ensure more secure voting systems for decades to come.** There are at least three types of grants that could further these goals:

[32] RONALD L. RIVEST & JOHN P. WACK, COMPUTER SCI. AND ARTIFICIAL INTELLIGENCE LAB. MASS. INST. OF TECH., CAMBRIDGE, MASS., ON THE NOTION OF "SOFTWARE INDEPENDENCE" IN VOTING SYSTEMS, (2006), *available at* https://people.csail.mit.edu/rivest/pubs/RW06.pdf.

[33] *Post Election Audits*, VERIFIED VOTING, https://www.verifiedvoting.org/resources/post-election-audits/.

[34] *Internet Voting*, VERIFIED VOTING, https://www.verifiedvoting.org/resources/internet-voting/ (last visited Sept. 26, 2016).

[35] NORDEN & FAMIGHETTI, *supra note* 3, at 10.

[36] Computer Technologists' Statement on Internet Voting, VERIFIED VOTING (2008), *available at* https://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf.

1. Grants to pilot testing and implementation of voting systems that use non-proprietary open-source software (defined as voting system where the software license is made available under an Open Source license), as well as commercial or custom firmware and hardware could lead to more secure and reliable systems nationwide.

   - A key challenge in ensuring more secure and reliable voting systems is cost
   - Many experts agree that the widespread use of open source systems using commercial off the shelf hardware could dramatically decrease the cost of upgrading and replacing systems and parts.[37]
   - Los Angeles County, California and Travis County, Texas are currently working to create such systems for their own voters. Grants to support the development of these programs, or start new ones, would increase the chance that this work could spread more quickly.[38]

2. Grants to create a common data format allowing for voting-equipment device interoperability could increase reliability and security.
   - The National Institute of Standards and Technology is doing work to create a common data format for elections.
   - If NIST (or another organization) could create a common data format allowing for voting-equipment device interoperability, it could result in a huge saving on voting system costs (jurisdictions could mix and match equipment), making needed upgrades and replacements more viable.

3. Grants to the EAC or state election agencies for training to local election officials on machine security, maintenance, pre and post-election testing, development of contingency plans in event of cyber-attack or failures, and poll worker training.

III. Conclusion: Integrity, public confidence and access are inextricably linked

For far too long, the integrity of our elections has been presented as antithetical to access to the ballot box. In fact, the two are inextricably linked. As the Brennan Center argues in a recent report, *Election Integrity: A Pro-Voter Agenda,* ensuring that all American citizens who want to participate in our electoral system can vote is not only critical for free and fair elections, but also the best way to ensure integrity and confidence in our system.[39] This is why the Brennan Center has opposed laws that limit access and the ability of eligible voters to cast ballots, but seem to

[37] ROBERT F. BAUER ET. AL, THE AMERICAN VOTING EXPERIENCE: REPORT AND RECOMMENDATIONS OF THE PRESIDENTIAL COMMISSION ON ELECTION ADMINISTRATION, PRESIDENTIAL COMM'N ON ELECTION ADMINISTRATION, JANUARY, 2015, *available at* https://www.supportthevoter.gov/files/2014/01/Amer-Voting-Exper-final-draft-01-09-14-508.pdf

[38] NORDEN & FAMIGHETTI, *supra note* 3, at 22-25.

[39] MYRNA PEREZ, BRENNAN CTR. FOR JUSTICE, ELECTION INTEGRITY: A PRO-VOTER AGENDA (2016), *available at* https://www.brennancenter.org/publication/election-integrity-pro-voter-agenda.

have little actual security benefit. As detailed in a summary by the Brennan Center 14 states will have new voting restrictions in 2016.[40]

Our aging equipment provides a clear example of how access and integrity are interdependent. Researchers from the Massachusetts Institute of Technology and Harvard estimate that in 2012 between 500,000 and 700,000 eligible voters did not vote because of long lines.[41] The longer we wait to replace antiquated machines, the more likely this problem will get worse.

This challenge impacts access for voters, of course, but also the integrity of our elections and public confidence in them. In a highly partisan age, where conspiracy theories can flourish on social media, and risks associated with foreign and domestic hacking are real if too often sensationalized, it is critical that we take necessary steps ensure that the public can will have confidence in election results, and that malfunctions or vulnerabilities do not lead fair minded citizens to question the accuracy of election results.

The 2000 election was a traumatic event for American confidence in our electoral system. It is disturbing to imagine how much more difficult that event would have been for the country had it been preceded by months of overheated rhetoric about rigged elections and Russian hacks.

The nation made important changes to the way we vote in response to the 2000 election crisis, including replacing problematic equipment like punch card voting machines. But the changes came later than they should have; critics had been warning punch card machines should be replaced since at least the 1970s.[42] We should not make the same mistake twice. Investment in the security and reliability of our voting systems should come *before* we experience another such crisis.

[40] *New Voting Restrictions in Place for 2016 Presidential Election*, BRENNAN CTR. FOR JUSTICE, http://www.brennancenter.org/voting-restrictions-first-time-2016.

[41] Charles Stewart III & Stephen Ansolabehere, *Waiting in Line to Vote* 8 (Caltech/MIT Voting Tech. Project, Working Paper No. 114, 2013), *available at* http://vote.caltech.edu/documents/27/WP_114.pdf.

[42] Jim Drinkard, *Holes in Punch-Card System Noted Long Ago*, USA TODAY, Mar. 7, 2001, http://usatoday30.usatoday.com/news/politics/2001-03-07-voting.htm.

Appendix A

BRENNAN CENTER
FOR JUSTICE
TWENTY YEARS

at New York University School of Law

ELECTION 2016
CONTROVERSIES

Voting System Security and Reliability Risks

The last few weeks have brought renewed attention to the security and reliability of our voting systems. After credible reports last month that Russia was attempting to influence American elections by hacking into the DNC email server and other campaign files, new reports show the FBI has determined foreign hackers penetrated two state election databases.

This fact sheet describes what the risks to America's voting system security really are — and what states, localities, and voters can do to prevent successful attacks against the integrity of our elections.

The Brennan Center has studied the use of computerized voting systems for over a decade. In a comprehensive study released last year, we found the use of outdated voting equipment across the country presents serious security and reliability challenges.

The United States has made important advances in securing our voting technology in the last few years. Relatively few votes are cast over the internet or machines connected to the internet,[1] and the vast majority of ballots will be cast on systems that have a paper trail that allows election officials to independently verify software totals. This makes it highly unlikely that a cyberattack against our voting machines could have a widespread impact on the results of a national election.

Still, there is much more we should do to promote the security and accuracy of our voting systems. Computer scientists have demonstrated that older equipment, in particular, can be very insecure. It is also more difficult to maintain, and more likely to fail (even without interference from an attacker) on Election Day. While small-scale attacks or failures of individual machines might not have a widespread impact on national vote totals, they can severely damage voter confidence, and would be particularly troubling in very close contests.

Similarly, while proper safeguards can ensure attacks on voter registration databases don't prevent a legitimate voter from casting a ballot or having her vote counted, an attack on these systems could put voters' personal information at risk. Election officials must take all steps necessary to protect such information.

In the short run, we should do everything we can to minimize the impact of such attacks or failures. In the long run, we must treat our election infrastructure like other critical infrastructure, with regular investments and upgrades.

***

[1] Several states allow military and overseas voters to cast ballots by fax, e-mail or internet portal. Alaska allows any qualified voter to request and return an absentee ballot via facsimile.

Before detailing how election security and reliability can be improved, it is important to understand the significant steps that have been taken to protect the integrity of our elections over the last several years.

Improvements to Election Security

- Today, 47 of 50 states rely on the Election Assistance Commission's (EAC) federal certification process when purchasing voting machines. This process includes much more rigorous security testing than previously existed.
- While recent hacks deserve our attention, the overwhelming majority of voting is not done over the internet.
- In recent years, voting machines that could be accessed remotely have been taken out of service,[2] making widespread, remote attacks much more difficult.
- Many jurisdictions have replaced their paperless machines with systems that scan paper ballots filled out by voters, or produce a paper trail that can be reviewed by the voter.
- This November, at least 80 percent of registered voters will make selections on a paper ballot, or vote on an electronic machine that produces a paper trail.

Despite these advances, there is still more work to do to ensure that all voting machines are as secure and reliable as possible.

Outdated Voting Machines Pose Serious Reliability and Security Risks

- In November, 42 states will use voting machines that are at least 10 years old. This is perilously close to the end of most machines' expected lifespan. Using aging voting equipment increases the risk of failures and crashes — which can lead to long lines and lost votes.
- Aging voting systems use outdated hardware and software. For this reason, replacement parts for older voting systems can be difficult, if not impossible, to find. Aging systems also rely on unsupported software, like Windows XP and 2000, which does not receive regular security patches and is more vulnerable to the latest methods of cyberattack.
- While nearly all of today's voting machines go through a federal certification and testing program, many jurisdictions purchased voting machines before this process was in place. Older machines can have serious security flaws, including hacking vulnerabilities, which would be unacceptable by today's standards.
- In November, some voters in 14 states will vote on paperless electronic voting machines. These machines do not produce a paper record that can be reviewed by the voter, and allow election officials and the public to confirm electronic vote totals.[3]
- While the need for more up-to-date, secure and reliable voting equipment is clear, funders at the state and federal level seem unconcerned about our aging voting infrastructure. In at least 31 states, election jurisdictions will need new machines in the next five years, but officials from 22 of those states said they did not know how they would pay for them.

[2] For instance, in 2015 Virginia decertified a voting system after finding that an external party could access its wireless features to "record voting data or inject malicious data." That system had been eliminated in Pennsylvania in 2007 and Mississippi in 2013, and is no longer in use anywhere in the United States.

[3] Delaware, Georgia, Louisiana, New Jersey and South Carolina use paperless electronic voting machines as their primary polling place equipment statewide. In Arkansas, Indiana, Kansas, Kentucky, Mississippi, Pennsylvania, Tennessee, Texas, and Virginia, some portion of polling places use such paperless machines as the primary equipment.

Short Term Solutions: Voters and Local Election Officials Can Enhance Security and Reliability

- Voters should vote early when possible, to avoid potential delays caused by machine breakdowns on Election Day.
- If voters experience problems while voting on machines, or if those machines fail, they should immediately report the problem to local officials or poll workers, and then call 866-OUR-VOTE, the Election Protection hotline, to report the problem.
- Election officials should report machine problems to the EAC so other jurisdictions using the same voting system are aware of potential issues.
- All state and local election officials should ensure the physical security of voting equipment and paper records at all stages of the process — whether in storage, in transit to polling places, or during an election — by implementing strong chain of custody procedures.
- All local election officials should conduct thorough pre-election testing on every voting machine and ensure emergency paper ballots are available at all places where electronic machines are used.
- All states should mandate thorough post-election audits to confirm that paper records match electronic results. Officials should also review and, where necessary, improve "reconciliation policies" to guarantee that the number of signed-in voters matches ballot totals, and that machine and polling place totals match county and state totals.

Long Term Solutions: State and Federal Action for Improving Security and Reliability

- Congress and state legislatures need to allocate the funds for new, reliable, and secure voting systems. Grants to fund voting technology improvements can ensure more secure voting systems for decades to come.
- Congress and state legislatures should require audits of election results, using paper ballots or voter verifiable paper records, to confirm electronic totals. Today, only 25 states require that election officials conduct paper audits.
- The next president and Congress must ensure the EAC has a full slate of commissioners and fill any vacancies in a timely manner. The work of the agency is critical to ensuring that local and state election officials have the best information to ensure our voting machines are secure and accurate.

Protecting the Integrity of Voter Registration Databases

- As long as states and local jurisdictions keep backups, including paper copies of their registration lists, no manipulation of state computer registration databases should prevent legitimate voters from casting a ballot, or having their votes counted.
- Voter registration databases can and should be programmed to run frequent, automated scans of registration activity to monitor for and alert election officials to potentially fraudulent or abnormal activity, such as a high volume of traffic or oddly timed traffic.
- Voter registration databases should be constructed to record transaction logs for all requests submitted to the site. This would allow officials to trace suspicious activity, or review activity after-the-fact for abnormal site traffic patterns.

- Websites providing online voter registration should employ best practices to protect against large-scale attacks, such as forcing an application to "time out" automatically after a certain period of inactivity, and using CAPTCHA tests.
- Voter registration databases should not contain any information other than what's required to register, or specified information relevant to the administration of elections.
- States should publish — and enforce — a policy detailing use limitations (including user authorizations) and security safeguards to protect voters' personal information in the data transfer process, the online or telephone interface, and the maintenance of the voter registration database.

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

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.

BRENNAN
CENTER
FOR JUSTICE

at New York University School of Law

For more information, contact Lawrence Norden at (lawrence.norden@nyu.edu, 646-292-8326) or Christopher Famighetti (christopher.famighetti@nyu.edu, 646-292-8387).

GUIDANCE FOR ELECTION OFFICIALS WITH AGING VOTING EQUIPMENT

Many jurisdictions around the country will be using equipment in 2016 that is rapidly approaching the end of its projected lifespan. Fortunately, there are steps election officials can take now to reduce the likelihood of problems on Election Day and beyond.

1. Review EAC Guidance on Reducing Machine Failures

The bipartisan EAC has published detailed guidelines on effective maintenance of aging equipment. Soon, they will also publish best practices for pre-election machine testing. Additionally, they offer tips for post-election audits and ballot reconciliation, which are critical in ensuring that equipment failures do not impact results.

2. Update Poll Worker Training

To prepare poll workers to respond effectively to possible Election Day problems, their training must cover common machine failures and their solutions. The Center for Civic Design for the National Science Foundation released a report noting that training should include explanation of Election Day checklists, as well as emphasis on their importance. These checklists should encompass both standard procedures and troubleshooting steps. Also important is giving poll workers hands-on practice, creating scenarios in training for them to react to, so that when the moment comes, they can act quickly and securely. Officials should consider forming teams of experienced poll workers who can act as first responders when something goes wrong in the polling place.

3. Prepare Contingency Plans

Particularly in jurisdictions that use DREs, it is critical that all polling places have enough paper ballots to use in the event of machine failures. Even in jurisdictions that use optical scan machines, plans should be laid to ensure that voters can cast votes securely, and without undue delay, if machine breakdowns occur.

4. Report Machine Problems to the EAC

Too often, election officials are not notified of machine defects or failures discovered by officials in other parts of the country – even when they use the same machines. The EAC should serve as a clearinghouse for such information, disseminating updates on emerging machine problems to officials nationwide. For this system to work better, state and county officials must promptly report to the EAC any problems they experience arising from aging voting machines.

5. Carefully Consider Equipment Purchases

The EAC has produced helpful suggestions for jurisdictions considering buying new equipment. Leasing is another option, one that the State of Maryland and some counties in Virginia have chosen. Linda Lamone, Election Director of the State of Maryland, and Edgardo Cortes, Elections Commissioner for Virginia could both speak to their experience with equipment leases.