PRINCETON UNIVERSITY

Department of Computer Science
35 Olden Street
Princeton, New Jersey 08540-5233

Andrew W. Appel
Eugene Higgins Professor of Computer Science

(609) 258-4627 appel@princeton.edu

Written testimony of Andrew W. Appel

House Subcommittee on Information Technology
hearing on "Cybersecurity: Ensuring the Integrity of the Ballot Box"
September 28, 2016

My name is Andrew Appel. I am Professor of Computer Science at Princeton University, where I have been on the faculty for 30 years and served 6 years as Chair of the Computer Science Department. In this testimony I do not represent my employer. I'm here to give my own professional opinions as a scientist and a technologist, but also as an American citizen who cares deeply about protecting our democracy.

My research and expertise is in software verification, applied computer security, and technology policy.

As I will explain, **I strongly recommend that, at a minimum, the Congress seek to ensure the elimination of "touchscreen" voting machines, immediately after this November's election; and that it require that all elections be subject to sensible auditing after every election to ensure that systems are functioning properly and to prove to the American people that their votes are counted as cast.**

Since 2003 a significant part of my research has been on the technology and security of the equipment we Americans use for elections: voting machines and election administration computers. On the topic of election machinery, I have written 5 scientific papers and 37 short articles, taught two courses at Princeton; and done expert forensic examinations and given sworn testimony in two court cases in New Jersey. In 2009 I demonstrated in open court, in the Superior Court of New Jersey, how to hack a voting machine.

There are cybersecurity issues in all parts of our election system: before the election, voter-registration databases; during the election, voting machines; after the election, vote-tabulation / canvassing / precinct-aggregation computers.

Let me start with a general principle: When we elect our government officials, sometimes we are voting for or against the very person or political party who is in office right now, running that very election! How can we trust that this person is running the election fairly? The answer is, we organize our elections so we don't have to trust any single person or party. That's why, when you go to the polls in most places, there are typically two pollworkers there, often (by law) from different political parties; and there are pollwatchers, representing the parties to make sure everything is done right. That's why recounts are done in the presence of witnesses from both parties. We run our elections transparently so the parties can watch each other, and the result is that even the losing candidate can trust that the election was run fairly.

In the U.S. we use two general kinds of voting machines: optical-scanners, and direct-recording machines (usually called "touchscreen" voting machines). In each voting machine is a computer, running a computer program. Whether that computer counts the votes accurately, makes mistakes, or cheats by shifting votes from one candidate to another, depends on what software is installed in the computer. Everyone in this room uses computers in their daily lives, and we have all had occasion to install new software. Sometimes it's an app we purchase and install on purpose, sometimes it's a software upgrade sent by the company that made our operating system, or word-processor program, or whatever. Installing new software in a voting machine is not really much different from installing new software in any other kind of computer.

In New Jersey I demonstrated exactly how to craft a fraudulent, vote-stealing computer program that would shift votes from one candidate to another. I did this in a secure facility and I'm confident that it has not leaked out to affect real elections, but really the software I built was not rocket science—any competent computer programmer could write the same code. Installing that vote-stealing program in a voting machine takes about 7 minutes, per machine, with a screwdriver. Once it's installed, it could steal elections for years to come.

Voting machines in New Jersey (and many states) are delivered to polling places several days before the election—to elementary school gymnasiums, churches, firehouses. These are not secure facilities, and anyone could gain access to a voting machine for 10 minutes. Also, the machines are stored in county warehouses: Let's assume that these county employees or private contractors have the utmost integrity, but still, in the U.S. we try to run our elections so that we can trust the election results without relying on any one individual.

I'm not the only one who's demonstrated how to hack a voting machine. Colleagues and students and Princeton University and elsewhere have demonstrated the same principle on several different models. This is not just one glitch in one manufacturer's machine, it's the very nature of computers. And some voting machines can be hacked without ever touching them, by means of computer viruses transmitted on ballot cartridges.

So how can we trust our elections when it's so easy to make the computers cheat? Forty states already know the answer: vote on optical-scan paper ballots.[1] The voter fills in the bubble next to the name of their preferred candidate, then takes this paper ballot to the scanner—right there in the precinct—and feeds it in. That opscan voting machine has a computer in it, and we can't 100% prevent the computer from being hacked, but that very paper ballot marked by the voter drops into a sealed ballot box under the opscan machine. That's the ballot of record, and it can be recounted by hand, in a way we can trust.

[1] Actually, in a few of these 40 states, they use "DRE with VVPAT," touchscreen machines equipped with a ballot printer so the voter can see that the paper record of their vote matches the selections they made on the touchscreen. This technology is not as good as optical-scan paper ballots, but I consider it adequate. DRE with VVPAT stands for "Direct Recording Electronic [voting machine] with Voter-Verified Paper Audit Trail." Overall, my count of 40 states is approximate--the reason is that many states use different equipment in different counties. If a state uses op-scans in almost all its counties, then I just count it as an op-scan state, and so on.

Paper ballots are even better protection against fraud with systematic auditing to make sure the computers aren't cheating. You don't have to recount every ballot box, just spot-check a statistical sample. There are 12 states that do this, by law; it's a good idea, and all states should do it.

It's not just malicious hacking or deliberate cheating that this protects against. Sometimes the machines are accidentally miscalibrated, or there's an unintentional software bug; these audits catch those problems too.

Even so, in most of those 12 states, the sampling methods are weak: newer auditing methods would give higher assurance that the results are accurate, *and* actually be cheaper and less labor-intensive to implement. And in many of those states, the rules are unclear for "how much discrepancy is enough to trigger a wider audit, or trigger a full recount?"

All states should pay attention to ballot chain-of-custody (who's had access to those ballot boxes between the close of the polls and an audit or recount?) and ballot accounting (how many votes were cast in each precinct? Does that match the number of ballots? -- but there's more to ballot accounting when early voting and vote centers are used).

Unfortunately, there are still about 10 states that primarily use touchscreen voting computers. There's no paper ballot to recount. After the voter touches the screen, we have to rely on the computer—that is, we have to rely on whatever program is installed in the computer that day—to print out the true totals that night when the polls close.

So what must we do? In the near term, we must remember not to connect the voting machines directly to the Internet. The reason is that almost all computer software has security vulnerabilities--software bugs that can be exploited by attackers. It takes enormous expertise and skill to run a secure computer network, and even then one cannot achieve perfect security in the face of a determined attacker. It's unrealistic to demand perfect cybersecurity from state and county election administrators.

And don't connect the election-administration computers to the Internet, either: those computers used to prepare the electronic ballot definition files before each election, that are used to program the voting machines. That is, we must not connect the voting machines even indirectly to the Internet. There are many able and competent election administrators across the country who already know this, who already follow this "best practice." I hope that all 9000 counties and states that run elections follow this practice, but of course it's hard to tell whether they all do.

This best practice can help to protect against hacking of voting machines by people in other countries through the Internet. But it can't really protect us from insider hacking, or against local criminals with access to the machines before or after elections. So what we must do as soon as possible after November is to adopt nationwide what 40 states have already done: paper ballots, marked by the voter, countable by computer if you like but recountable by hand.

In 2000 we all saw what a disastrously unreliable technology those punch-card ballots were. So in 2002 the Congress outlawed punch-card ballots, and that was very appropriate. I strongly recommend that the Congress seek to ensure the elimination of Direct-Recording Electronic, that is, "touchscreen" voting machines, immediately after this November's election.

Other recommendations:

Now let me turn briefly to *before* the election: voter registration databases; and *after* the election, canvassing/aggregation computers.

This month the EAC distributed to State election directors these memos:

Best Practices for Continuity of Operations (Handling Destructive Malware),
by ICS-CERT, Department of Homeland Security, 1/22/2015.

Ransomware and what to do about it [and related memos],
from DHS / DOJ / HHS, etc.

Security Tip (ST16-001): Securing Voter Registration Data,
from US-CERT, Department of Homeland Security.
https://www.us-cert.gov/ncas/tips/ST16-001

The information in these documents is generally accurate, expert, informative, and useful. I expect it will be helpful to election administrators. In fact, those election administrators who have not been "up to speed" on these best practices will have a lot of work to to! But *all* of these manuals are generic cybersecurity-administration advice, none of it specific to elections.

Therefore, I suggest these recommendations as an election-specific supplement to the DHS's advice:

> **Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections**, edited by John McCarthy, Stephanie Singer, Lawrence Norden, Whitney Quesenbery, Mark Lindeman, Andrew Appel, Kim Alexander, and Joe Kiniry, September 5, 2016.
> https://electionverification.org/wp-content/uploads/2016/09/evntop109516.pdf

We focus not on pure cybersecurity, but on how to achieve trustworthy elections even with fallible computers. I attach this document to my testimony, and here I'll mention just one or two points.

We can't just disconnect voter-registration computers from the Internet; there's a legitimate role for the Internet in serving voters this way, following appropriate state laws. But on the other hand it's very difficult to make any computer perfectly secure against hackers on the Internet. If voters are removed from the registration list by hackers, that can cause disenfranchisement. I'm particularly concerned about pollbooks. When you show up to vote, the pollworker checks your name, address, and signature in a pollbook. In those jurisdictions where the pollbooks are electronic (running on laptop or tablet computers), I'm

particularly concerned that hacks could disable these on election day, causing chaos. So election administrators must follow best practices, such as the ones cited above, to make sure they have backups and contingency plans.

When the polls close on election night, the vote totals in each voting machine—in each precinct—are transmitted to some central computer—let's call it "county central"—where all the precincts can be added together. It's a best practice not to do this through the Internet; in New Jersey I believe they have one Democratic pollworker and one Republican pollworker transport the electronic ballot cartridge, along with a paper printout from the voting machine signed by witnesses in the polling place, to county central. But how can we trust that the electronic ballot cartridges are not hacked, or the county central computers?

The answer is that we set up our elections so that these computers don't need to be trusted; of course we protect them from hacking as best we can, but even if they are hacked, the citizens and candidates can be sure of the election results. We do this—already—as follows: in each precinct when the polls close, the vote totals in that precinct are announced right there, to all witnesses present: pollworkers, party pollwatchers, and citizens. That's the law in most states, and that's actually the practice in most states. These pollwatchers can take these numbers back to their party's victory party, or whatever, and compare the per-precinct numbers to the table reported by the County Clerk. And they can add up all the precincts themselves, and compare with the county-central computer. I recommend that this admirable practice, already the law in most places, should be encouraged and supported by election administrators, who have nothing to hide in the way that they run our elections.

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.

PRINCETON UNIVERSITY

Department of Computer Science
35 Olden Street
Princeton, New Jersey 08540-5233

Andrew W. Appel
Eugene Higgins Professor of Computer Science

(609) 258-4627 appel@princeton.edu

Biographical Sketch

Andrew W. Appel is Eugene Higgins Professor of Computer Science at Princeton University, where he has been on the faculty since 1986. He served as Department Chair from 2009-2015. His research is in software verification, computer security, programming languages, and technology policy. He received his A.B. *summa cum laude* in physics from Princeton in 1981, and his PhD in computer science from Carnegie Mellon University in 1985. He has been Editor in Chief of *ACM Transactions on Programming Languages and Systems* and is a Fellow of the ACM (Association for Computing Machinery). He has worked on fast N-body algorithms (1980s), Standard ML of New Jersey (1990s), Foundational Proof-Carrying Code (2000s), and the Verified Software Toolchain (2010s). He is currently the Principal Investigator of a major NSF-funded project, *The Science of Deep Specification.*

Professor Appel is the author of more than 125 scientific papers and books. On the topic of elections and voting technology he has written 5 scientific papers and 37 short articles, given expert testimony in 2 court cases, and taught 2 semester-long courses on "Election Machinery" at Princeton University.

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name: Andrew W. Appel

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

Principled Optimizing Compilation of Dependently Typed Languages, National Science Foundation grant CCF-1407794, $600,000, 2014-17.
Collaborative Research: Expeditions in Computing: The Science of Deep Specification, National Science Foundation grant CCF-1521602, $3,453,419, 2015-20.
(I am Principal Investigator on these grants, which are not made to me personally but to Princeton University)

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

None.
(I am employed by Princeton University, but I am not testifying on behalf of Princeton University.)

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

I certify that the above information is true and correct.
Signature: Andrew Appel Date: 9/15/16