Testimony to the Election Assistance Commission

Technical Guidelines Development Committee (TGDC)
Public Data Gathering Hearings
September 20, 21, 22, 2004
National Institute of Standards and Technology, Gaithersburg, Maryland

Jim Adler
Founder, VoteHere, Inc.

TECHNOLOGY IS AVAILABLE TODAY FOR SECURE AND VERIFIABLE ELECTRONIC ELECTIONS

Thank you members of the technical guidelines development committee for inviting me here today.

Of course, the bad news about Election 2000 was that mainstream America, for the first time, realized that elections were not perfect. In fact, as the CalTech/MIT Voting Technology Project reported, 2 million ballots were lost due to the mechanics of voting – be it, punch card, lever machine, optical scan, or touch-screen. The good news is that we are now focused on innovating election technology to solve these complex issues.

So far we've heard a bipolar security debate between, on the one hand, "electronic voting machines are fine as-is" and, on the other, "the only way forward is to go back to paper ballots." Many people agree there is a problem with electronic voting today. However, we don't all agree that the CPR (contemporaneous paper record, or voter-verified paper ballot) is the best solution because we already know paper ballot-based systems are badly flawed. I am here to tell you that there is a third way – a better solution to prove that every vote is counted properly without falling back to paper ballots – the same paper ballots that have been at the root of electoral fraud and disenfranchisement throughout our history.

There are technologies available today (VoteHere's VHTi is one of them) that can make electronic voting better than paper ballots and still retain all the accessibility and operational benefits of electronic voting machines. Just because some people have diagnosed the electronic voting machine disease doesn't mean that the only cure is going back to paper ballots. There are other cures.

The call for paper ballots is similar to the call nearly 100 years ago to ban the automobile and go back to horses. Back then, the automobile was considered dangerous new technology lacking critical safety equipment such as safety glass. Instead of moving backward in elections, we need to look forward and in effect add "safety glass" to our electronic voting machines.

Today I'll outline technology that brings measurable certainty and transparency to every election – from the voting booth to the final election results, solves the current dilemma, and is available now (others are also available in the market today). My message to you is very simple: we should let innovation (and HAVA and NIST) work and not revert back to paper ballots, which have historically failed us.

ABOUT VOTEHERE

To provide context for my remarks, let me tell you a little bit about me, and the company I founded in 1996. VoteHere was born as a data-security company developing cryptographic software for encryption and digital signatures. We focused our expertise exclusively on electronic voting starting in 1998. In 1999, I served on the California Internet Voting Task Force. Currently, I co-chair the IEEE Special Task Group on Voter-Verifiability (P1583, STG3), where we have discussed e-voting security at great length. Before founding VoteHere, I worked on mission critical avionics systems for space launch vehicles. I've learned that this early training in mission-critical systems prepared me well for the more terrestrial mission-critical world of elections.

Over the last five years, VoteHere's Chief Scientist, C. Andrew Neff, has developed cryptographic protocols for conducting secure electronic elections that retain the secret ballot. Dr. Neff's work has been profiled at industry conferences and by the *Society for Industrial and Applied Mathematics*. Currently, MIT Professor Ron Rivest is teaching cryptography coursework using Dr. Neff's protocols for secure electronic voting. As many of you know, Professor Rivest is a cryptography pioneer, Turing Award winner, member of the CalTech/MIT Voting Technology Project, and has recently been appointed to the EAC Board of Advisors.

VoteHere is fundamentally a software company. We don't make electronic voting machines. We make software that goes inside electronic voting machines. Our technology proves, in every election, that electronic voting machines (and backend tabulation databases) aren't cheating or making mistakes, and provides for a meaningful audit.

At VoteHere, we understand mission critical applications, are world-class leaders in cryptography, and have advanced the state of the art in electronic voting. In many crucial ways, VoteHere represents the emerging face of innovative election technology.

Last summer, we announced a non-exclusive agreement with Sequoia Voting Systems to integrate our technology into their electronic voting machines. Today, we have announced a non-exclusive alliance with Advanced Voting Solutions (AVS), a cutting-edge manufacturer of electronic voting machines. We plan to test our technology inside AVS's voting machines in the upcoming Fall elections. We are also in discussion with all of the other voting machine manufacturers and election officials who have expressed strong interest in deploying our technology.

IN EVERY ELECTION, VHTi PROVES THE TRUST PLACED IN ELECTRONIC VOTING

VoteHere has a solution called VHTi, a voter verified election audit technology that works inside any electronic voting machine. VHTi is an audit system that sits inside the electronic voting machine. Even though software, hardware, and procedures may be opaque, the audit system is 100% transparent and will, with certainty, detect if a single ballot is corrupted, either maliciously or accidentally.

VHTi goes beyond VVPB because it proves election results are valid end-to-end, not just at the polling booth. VHTi does two basic things. First, VHTi gives voters a voter verified receipt to check both that their vote was properly recorded at the poll site and properly counted in the final results while maintaining ballot secrecy throughout (see attached). Second, VHTi enables a meaningful and transparent audit trail that lets anyone independently verify the election results with accuracy down to a single vote.

VHTi and similar technologies on the market today go beyond paper ballots by allowing voters to verify, not just that their vote was recorded (as paper ballots claim to do) but, that their vote actually got counted (which paper ballots absolutely cannot do) – even when faced with hackers, malicious software, procedural missteps, and software bugs that may compromise their ballot along the way – all without reintroducing the known weaknesses of paper ballots or violating ballot secrecy.

The effectiveness of our technology does not rely on securing software source-code or hardware, but instead on the transparent audit process it enables. It does not protect elections from compromise but detects when elections are compromised – whether by hackers, corrupt insiders, or software bugs. Too often security experts have misunderstood elections as only being secured by *protective* measures, like big fences you might build around your house. Elections have always been secured by *detecting* election problems when they occur, like guard dogs who alert you to intruders or problems inside your house.

Yes, it is always good to build big fences, but it is just as critical to have a guard dog that barks when intrusions inevitably occur. By providing voters the ability to verify that their vote was counted and providing third parties the ability to verify election results, VHTi is that guard dog.

As a practical matter, tracking our votes is really as simple as tracking a package sent by the U.S. Postal Service or tracking a lottery ticket to its point of purchase. Everyday, using simple tracking codes, Americans verify the delivery of 12 million packages. If we can know the destiny of our packages, why can't we know the destiny of our votes? Well now we can.

The oft-used reason for not using a true receipt that could be taken home is that it could violate a voter's privacy and be used for vote buying or voter coercion. VHTi provides an encrypted receipt to assure the voter that her vote was counted properly but cannot be used to pass that assurance on to anyone else. I realize that this capability may sound unbelievable, but this is the type of long overdue innovation that we're now embarking upon – in no small part due to HAVA.

Providing voters an opportunity to verify their vote provides tremendous advantages for *detecting* election problems. Statistically, it turns out that even if a small number of voters faithfully verify their ballot, any election anomaly would be detected with near certainty (see the Appendix A for more detail). If *anything*—man or machine—interferes with a ballot *anywhere* from the time it leaves the voter's brain to the time it is tallied in the final election results, its detection would be guaranteed and could be proven in court.

Those who argue that a "paper ballot" is *the only way* to audit or recount an electronic election miss two commonly accepted practices. First, computer forensics often relies on all-electronic evidence. Everyday, this practice withstands legal challenge, assuming adequate maintenance of the chain of evidence. Second, lever machine recounts have been conducted for more than 100 years without paper ballots. Lever machine recounts have earned the trust of the electorate by a system of verification checks on the machinery, typically to ensure a trusted chain of custody.

The Help America Vote Act (Title III, Subtitle A, Section 301.a.2.B.i) already requires voting systems to print paper ballots for a recount, typically after the polls close. This has been criticized on the grounds that it makes little sense to print the ballots *after* the election if the voting machine is not trusted to record them correctly in the first place. VHTi provides a means to prove the trust placed in voting machines, through its voter-verified receipt, so that printing of voted ballots after the election can be trusted.

HOW VHTi WORKS

Briefly, here's how it works (this demonstration is also available at http://www.votehere.com/downloads.html):

Just like at the gas pump, the voter has the *option* to obtain a detailed receipt of each race she wishes to verify. A random tracking code is built by the machine and by the voter for the voter's chosen candidate. This tracking code and its connection to the vote choice is shown to the voter in the privacy of the voting booth, but the receipt shows all of the candidates in order to mask the voter's choice. In this way, the receipt cannot be used to *prove* how she voted outside of the polling place. After the election, the receipt data is regenerated from the counted ballots and she can look up her receipt on the county website (or county office or election hotline) to verify that the receipt that she obtained in the polling place is the same that got counted.

While the county tallies the votes, the public can tally them independently as well. Nonpartisan watchdog groups (such as the League of Women Voters) could verify the results independently to ensure that no votes were lost or changed. Since all of the ballots are published into an entire election transcript, voters can do their part to verify their own vote and then anyone can verify the backend ballot box to verify that the count is right. In this way, voters have confidence that their own vote is in the final results because those results have been independently verified as a whole.

With so much transparency and with so many people monitoring the results, you can statistically guarantee that anomalies will be caught.

What's most attractive about this type of voter-verified receipt is that it acts as a "spot-check" on the election system. Much of the criticisms have focused on the fact that we have no way to justify the trust we place in electronic elections. The encrypted voter-verified receipt allows voters to spot-check the election system with a degree of statistical confidence that guarantees the eletion results are valid.

In Appendix A, I provide a standard that defines a measurable "margin of error" on the election results that applies even when faced with accidental and malicious errors in hardware, software, and procedure. This standard has been submitted to California's Secretary of State, Kevin Shelley; to the IEEE Voting Equipment standard; and to the EAC. Any election system, whether paper or electronic, should be held to this standard.

TRANSPARENCY IS CRUCIAL FOR ELECTION CONFIDENCE

Finally, I'd like to talk about transparency.

Elections have always been safeguarded by transparent third party audit. Voters generally do not understand how a lever machine works, or how a punch card system works, or how a ballot is optically scanned. However, they trust that authorities, party observers, and watchdog groups will scrutinize both the mechanism and the process of our elections. The transparency that enables the scrutiny is what's important to voter confidence.

To that end, and since VoteHere's founding, we have recognized the importance of this openness. And, being good students of cryptography, we understand that there is no security in obscurity. After all, if I hide my money by burying it in my backyard, I may think it's safe, but most would agree that it is not really secure. VoteHere began a full-disclosure process in 1999 by filing (and as a result, publishing) the underlying VHTi technology patents. In September 2003, we publicly released detailed technical documentation. And earlier this month, we released the full source-code that implements the VHTi technology for public and scientific scrutiny, along with a sample implementation.

The use of cryptography is NOT just another "trust me" technology. In fact, exactly the opposite – it is a "trust no one" technology. In every election, absolutely everything connected with how every vote is handled end-to-end is published absolutely for scrutiny. Let me be clear: the software code is published, the cryptographic protocols are published, and all the election data is published. It's all laid out in the open. This lets ANYONE independently verify the results of the whole election. And every voter can verify that their vote was counted properly in the final results. Cryptography REDUCES the need to trust election officials, hardware, software, procedures, and vendors.

Paper ballots cannot do that. Paper ballots let voters check that their vote was recorded at the poll-site (if they check them at, which I'll discuss in a moment), but then it drops into a "black box" for the rest of the process. With paper ballots, we are forced to trust that our votes are handled properly beyond the poll-site.

Because, with paper ballots, the paper is the official source document, it is expected that only a very small percentage will check the paper under glass with the on-screen ballot. In a contested election, the paper ballot box will be impugned because the vast majority of voters are not looking at these supposed "source documents." However, if the voting machine produces a receipt, everyone need not ask for one. A small sample will detect problems. If they're ballots, every voter must scrutinize them, and carefully. We presented a statistical analysis on this issue at last December's NIST conference (see http://votehere.com/2003_12_01_jimadler_archive.html#107801943567893232).

CONCLUSION

The real fundamental axioms in this debate are:

(1) Voter-verification that allows a voter to ensure their individual vote is counted properly;

(2) Public verification of election results as a whole; and

(3) Transparency into the election process so that (1) and (2) occur in each election.

These fundamental axioms prove that the election technology and procedures didn't cheat or make mistakes, and election results can be meaningfully audited. With technology such as VHTi, we can prove these axioms in every election.

This is the promise of electronic voting – not just that electronic voting can be as good as paper, but that electronic voting can be better than paper. Frankly, the calls for better security, confidence, and transparency are necessary and we wholeheartedly embrace them.

But let's not be distracted by the call for paper ballots and be tempted to bring back the "horse and buggy". Instead of banning technology in elections, we should let innovation work and add "safety equipment" to our electronic voting machines. Only then will we have truly safe elections.

Elections have never been perfect but we should encourage the "pursuit of perfection." Today, I've discussed standards and technology to guide and measure how well we are doing. HAVA has empowered the EAC and NIST to do set those standards and perform those measurements. To resolve our current election dilemma, I urge you to keep the door open to innovation that will allow us to pursue perfection for the benefit all voters.

Thank you for your attention and I'd be happy to answer any questions.

APPENDIX A: RECOMMENDED STANDARD FOR MEASURABLE ELECTION CONFIDENCE

As co-chair of the IEEE Special Task Group on Voter-Verification (P1583, STG3), we have discussed voter-verification at great length. Although a contemporaneous paper replica (CPR, the so-called VVPAT or VVPB) may be configured to produce a measurable level of confidence in election results, your currently drafted standards have no such specification.

I would ask that you consider standard language that defines a measurable "margin of error" on the election results that applies even when faced with accidental and malicious errors in hardware, software, and procedure. Any election system, whether paper or electronic, should be held to this standard.

This approach was discussed at December's *NIST Symposium on Trust and Confidence in Election Systems*.[1] Furthermore, David Jefferson, a member of the California Touch Screen Task Force and current member of the California Voting Systems and Procedures Panel (VSPP), recommended this analysis as "a quantitative analysis of the effectiveness of voter verification and random precinct recounts in discovering errors or fraud."[2]

Here is proposed language for such a verification system as proposed to IEEE P1583, STG3:

1. The verification system must produce a measurable level of confidence in the election results, without violating any privacy requirement. From voter intent to election result, the Margin Of Error shall be 1% (or less) with 99% (or higher) level of confidence for all federal and statewide races.
2. The Margin Of Error shall be demonstrably proven for each election, even in the presence of accidental errors and malicious fraud, including those in hardware, software, and human procedure.
3. Any verification capability shall preserve voter privacy, so that it is not possible to ascertain that any vote within a precinct is more likely than any other to have been cast by a particular voter. Specifically, this means that one has to obscure, for each ballot:
    - What time the ballot was cast;
    - On what machine the ballot was cast;
    - In what language the ballot was cast;
    - Whether the ballot was cast through a disability interface;
    - Whether the ballot was provisional;
    - Whether the ballot was an absentee or vote-by-mail ballot;
    - Or any other property that helps identify what voter might have cast the ballot.

WE NEED MEASURABLE CERTAINTY TO BRING CONFIDENCE TO ELECTIONS

A logical question would be, "how many voters must verify to safeguard the election?" Well, before I get to that question, let me digress for moment.

Before Election 2000, many believed that elections were perfect. This idyllic belief was shattered in many respects and we, as an industry and society, have struggled with that reality. Without defining and quantifying confidence, we are in an uncomfortable place where we are tempted to manage perceptions rather than scientifically provable realities.

Let me give you a stark example of the danger in letting perception and fear tactics override scientific proof. In the mid 17th Century, the Black Plague struck Edinburgh, Scotland and thousands were dying from the disease. The city council was politically pressured to act. So, at one of the town meetings, with no science to support the decision, the council concluded that cats were responsible for the spread of the plague, and so ordered them all slaughtered. This was bad policy considering that cats made excellent rat catchers, and rats carried the fleas that carried the plague bacteria. As you've already guessed, by killing the cats, the city council caused the rat population to skyrocket along with the plague. The punch line, of course, is that you'd better have a firm grasp on the science that drives an intended outcome.

I don't mean to compare elections to the Black Death, but without applying clear science, we are being tempted into similarly bad policy.

For example, consider California Election Code 15360, which requires at least 1% of the precincts to be randomly chosen for hand recount. This statute is often given as a justification for CPR, but statistically it turns out that 60%, or 150,000 votes (in a typical Congressional district election of 250,000 votes) could be changed without detection by the 1% hand recount. This is just an application of the basic statistics that governs the "margin of error" in political polls.

---

[1] http://realex.nist.gov/CONFERENCES/Voting/DayOne/session2.5/adler.pdf

[2] http://lists.hss.caltech.edu/pipermail/votingtech/2003-December/000507.html

However, by allowing voters to verify that their votes were counted, a high level of confidence can be achieved with relatively few voters participating – like 2,000 out of 500,000. This is the punch line, so let me say it again: *if 2,000 voters faithfully verify their vote, the margin of error drops from 60% to less than 0.50%* – and the more voters that verify, the lower the margin of error.

This voter verification coupled with third party audit, proves that the entire election is *quantifiably* worthy of the trust we place in it – from voter intent to tabulated result. Malicious software, bugs, or errant procedures cannot touch the ballots without detection – that is, without the dog barking.

APPENDIX B: COMMENTS ON THE CONTEMPORANEOUS PAPER RECORD (CPR)

We should have learned by now that elections are deceptively difficult to fully grasp. We don't know that the CPR (the contemporaneous paper replica, also known as the voter-verified paper ballot) "paper pill" will cure the ills of electronic voting machines. Would we mandate a new untested drug that prevents cancer and require everyone to take it? Of course not. Well this "paper pill" is not yet specified; it has not been tested in the lab; and has not been tested in trials. Yet why are we considering requiring it?

Consider this scenario: My 64 year-old mother has been using touchscreen voting machines in Florida for the last few years. With the call for CPR, I explained how they would work with her current voting machine:

> She checks, before the ballot is cast, that what is printed on the paper matches what is on the touchscreen, which is what she intended to vote. The current prototypes would not let her touch the paper ballot but would only allow her to view it through a glass pane for comparison with the on-screen electronic version. Once she is satisfied that the paper ballot is identical to the on-screen electronic version, she touches the button to cast her ballot.

She then asked an interesting question: "Would my vote still count if I didn't compare the on-screen ballot to the [CPR] paper ballot?" I reassured her that, of course, her vote would still count. She then commented that it was unlikely that she would look over at the paper ballot since her attention was focused on the screen.

Fast forward to a contested election where the "paper ballot box" differs from the "electronic ballot box." There are many ways for this to happen including procedural and machine fault. The losing candidate of the "paper ballot box" brings voters, like my mother, into court that testify that they never looked at the paper ballot. This casts more suspicion on the election.

The moral is that CPR may provide a good way to detect problems with electronic voting machines, but it doesn't necessarily provide a reliable mechanism for recount.

Given millions of ballots, it is inevitable that the CPR count will disagree with the machine count in a close election. In that case, we won't know which ballot box to use. It's like having two wristwatches – when the watches disagree, what time is it? A root cause of problems during Election 2000 was ambiguity in what constitutes a vote – that is, whether punch card chads were pimpled, dimpled, pregnant, or hanging. Additional ballot boxes may seem like a good thing but a likely unintended consequence would be an ambiguous election result.

I understand the election-year intensity surrounding this issue, but before we use the blunt instrument of legislation to impact elections for a generation, shouldn't we make sure the CPR " paper pill" isn't a placebo and is actually safe and effective?

We shouldn't restrict ourselves to paper as the only way to achieve confidence and proof in our elections. There are better ways than taking the "paper pill."