

05hr\_SC-LEPR\_sb0296\_pt01



(FORM UPDATED: 08/11/2010)

## WISCONSIN STATE LEGISLATURE ... PUBLIC HEARING - COMMITTEE RECORDS

### 2005-06

(session year)

### Senate

(Assembly, Senate or Joint)

## Committee on Labor and Election Process Reform...

### COMMITTEE NOTICES ...

- Committee Reports ... **CR**
- Executive Sessions ... **ES**
- Public Hearings ... **PH**

### INFORMATION COLLECTED BY COMMITTEE FOR AND AGAINST PROPOSAL

- Appointments ... **Appt** (w/Record of Comm. Proceedings)
- Clearinghouse Rules ... **CRule** (w/Record of Comm. Proceedings)
- Hearing Records ... bills and resolutions (w/Record of Comm. Proceedings)  
(**ab** = Assembly Bill)                      (**ar** = Assembly Resolution)                      (**ajr** = Assembly Joint Resolution)  
(**sb** = Senate Bill)                      (**sr** = Senate Resolution)                      (**sjr** = Senate Joint Resolution)
- Miscellaneous ... **Misc**

# Senate

## Record of Committee Proceedings

### **Committee on Labor and Election Process Reform**

#### **Senate Bill 296**

Relating to: electronic voting system standards.

By Senators Plale, Carpenter, Erpenbach, Grothman, Hansen, A. Lasee, Olsen, Reynolds and Risser; cosponsored by Representatives Pocan, Freese, Ainsworth, Berceau, Black, Grigsby, Gunderson, Kessler, Lehman, Lothian, Molepske, Musser, Nelson, Parisi, Pope-Roberts, Richards, Seidel, Sheridan, Sherman, Shilling, Sinicki, Townsend, Travis, Wood and Gundrum.

August 24, 2005      Referred to Committee on Labor and Election Process Reform.

November 29, 2005    **PUBLIC HEARING HELD**

Present:    (5)    Senators Reynolds, Lazich, Kanavas, Hansen and Carpenter.  
Absent:    (0)    None.

#### Appearances For

- Jeff Plale — Senator

#### Appearances Against

- Anthony Buldin, Milwaukee — Voting Technologies International
- Brandon Scholz, Madison — Voting Technologies International

#### Appearances for Information Only

- Kevin Kennedy — State Elections Board

#### Registrations For

- Cynthia Poe, Madison
- Amilian Huesmann, Madison
- Paul Reckmer, Madison
- Lauren Vedal, Madison
- Jacqueline Scott, Madison
- Sofia Brichford, Madison
- Brian Juchems, Madison
- Deborah Renard, Shorewood
- Jaqueline Lindo, Mequon
- Eric Anderson, Madison
- Julien Colvia, Madison
- Molly Todd, Stoughton
- Liberty Karp, Madison
- Peter Brinson, Madison
- Mary Ebeling, Madison
- Mark Supanich, Madison
- Aubin Maynard, Madison

- Tim Carpenter — Senator
- Suzanne Leonard, Milwaukee
- Libbie Freed, Madison
- Beverly Speer, Madison
- Brian Tanner, Madison
- Donna Vukelich, Madison

Registrations Against

- Donna Bowen, Milwaukee — Voting Technologies International
- Bill Benning, Hartland — Voting Technologies International
- Dan Ross, Madison

May 4, 2006

Failed to pass pursuant to Senate Joint Resolution 1.

Patrick Henneger  
Committee Clerk



**Jacque, Barton**

---

**From:** Michael Kerr [mkerr@itaa.org]  
**Sent:** Tuesday, November 29, 2005 7:38 AM  
**To:** Sen.Reynolds  
**Cc:** Sen.Lazich; Sen.Kanavas; Sen.Hansen; Sen.Carpenter  
**Subject:** ITAA Letter in Opposition to A.B. 627 and S.B. 296  
**Importance:** High  
**Attachments:** ITAA Letter to WI Senate Labor & Election Process Reform - 11.29.05.pdf; FINAL infographic.pdf

Chairman Reynolds:

I am writing on behalf of the members of the Information Technology Association of America (ITAA) and its Election Technology Council. ITAA is the oldest and largest trade association for America's information technology industry. Our 400 corporate members provide IT products and services to governments around the world, to every federal civilian and defense agency, and every state government in the United States.

I have attached a letter conveying our opposition to **A.B. 627** and **S.B. 296**, bills providing, in part, new software coding disclosure and escrow requirements for electronic voting systems. We believe the coding disclosure requirements in this proposed legislation are unnecessary, given the current rigorous and objective regimen of voting system testing and certification at the federal and state levels. A graphic providing an overview of those processes is attached. Further, public source code disclosure may create new security risks for Wisconsin elections and may make Wisconsin voting systems procurements less competitive, as vendors will ~~be~~ deterred by a risk to their proprietary software.

Thank you for considering our comments and I would be happy to follow up with you or your staff to discuss our concerns. I can be reached at 703.284.5324 or [mkerr@itaa.org](mailto:mkerr@itaa.org)

Sincerely,

Michael Kerr

Cc: Members of the Senate Committee on Labor and Election Process Reform

---

**Michael Kerr** | Director, Election Technology Council  
Information Technology Association of America  
1401 Wilson Blvd., Ste. 1100 | Arlington, VA 22209  
office: 703-284-5324 | fax: 703-525-2279  
email: [mkerr@itaa.org](mailto:mkerr@itaa.org) | [www.itaa.org](http://www.itaa.org)

*Dedicated to promoting and growing your IT business.*

11/29/2005



November 29, 2005

The Honorable Tom Reynolds  
Chairman  
Senate Committee on Labor and Election Process Reform  
Room 306 South  
State Capitol  
Madison, Wisconsin 53707

Dear Chairman Reynolds:

I am writing on behalf of the members of the Information Technology Association of America (ITAA) and its Election Technology Council. ITAA is the oldest and largest trade association for America's information technology industry. Our members provide Information Technology (IT) products and services to governments around the world, to every federal civilian and defense agency, and every state government in the United States.

I am writing to convey our opposition to A.B. 627 and S.B. 296, bills providing new software coding disclosure and escrow requirements for electronic voting systems. In part, the legislation requires coding for software that is used to operate such systems to be publicly disclosed. The bills will also require each municipal clerk or board of election commissioners of a municipality that uses an electronic voting system to provide to any person, upon request, the coding for the software that the municipality uses to operate the system and to record and tally the votes cast.

The ITAA and its members urge you to significantly modify or remove the provisions relating to source code disclosure from this legislation. The provisions are both unnecessary and unlikely to deliver the intended outcomes. Indeed, the adoption of such requirements may create several negative outcomes for the state, which are discussed in the following paragraphs.

The provisions will not improve the efficiency or effectiveness of voting systems software inspection. Additional inspection and review of code by technical laypersons, with no ability to provide regulated feedback into the state election management process, is unlikely to improve the quality or security of the software. Our members would hold that current review processes allow all certification officials with a valid need to examine the software in a voting system to inspect that software. Such inspection is part of the established federal and state regimen of testing and certification for voting systems, which takes into account the election environment in which the system operates. To provide an overview of the complex and thorough federal and state testing requirements, ITAA developed a process flow diagram. The diagram, which we sent to Committee e-mail accounts this morning, illustrates the intensely-regulated independent testing and federal and state certification approval system that limits and controls the introduction of software and hardware improvements in the election environment.

Beyond the federal and state certification processes, the U.S. Election Assistance Commission (EAC) last year called on all voting systems vendors to voluntarily submit the executables of their proprietary voting system software to the National Software Reference Library (NSRL) to create a software repository from which state and local election administrators could verify the versions of software delivered to them. The voting system vendors agreed. Today, the NSRL contains voting systems software for most types of electronic voting systems used in this country.

The provisions in the bills under consideration will do more harm than good to the security of Wisconsin elections. A single-minded focus on the quality of software code will not improve the overall election security picture in the state. In fact, it may be detrimental to security. Today, a vulnerability in voting systems software can be recognized and mitigated in a well-managed election environment. However, the injection of a new vulnerability exposed to a larger pool of attackers will magnify the potential for risk.

Another poor outcome will be the harm done to the voting systems business of several major American software concerns, including those who have served the State of Wisconsin, and its counties and cities, loyally for years. Vendors faced with a mandate to divulge their Intellectual Property, a core asset of any IT business in which significant investment has been made over many years, will see a reduced incentive to compete for the State's business. Ours is a free-market system and those states creating greater risk for vendors, or placing restrictions or barriers on their voting systems markets, are making those markets less attractive. Vendors may elect to look elsewhere for lower levels of risk.

Ultimately, this legislation presents many unanswered questions and creates many concerns for vendors and elections officials, without delivering a tangible benefit to the vast majority

of the people of Wisconsin. Again, we urge you to reconsider and revise the provisions relating to software code disclosure. We would be happy to discuss our concerns with you and your staff at any time. Michael Kerr, Director of ITAA's Election Technology Council, is the staff contact and can be reached at 703.284.5324 or [mkerr@itaa.org](mailto:mkerr@itaa.org).

Thank you for considering our comments.

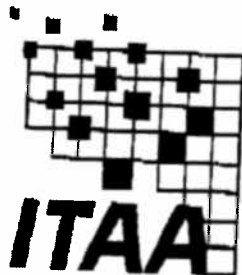
Sincerely,



Harris N. Miller  
ITAA President

Cc: Members of the Senate Committee on Labor and Election Process Reform





**Information Technology Association of America  
Enterprise Solutions Division**

**Facsimile Cover Page**

**FROM:** Michael Kerr  
Director, ES Division  
ITAA

**Direct:** 703-284-5324  
**Fax:** 703-525-2279  
**Email:** mkerr@itaa.org

**TO:** Chairman Tom Reynolds

**ORGANIZATION:**

**FAX #:** 608-267-0367 **PHONE #**

**DATE:** 11/29/05 **PAGES:** 4

**SUBJECT:**

**MESSAGE:**

Visit us on the World Wide Web at:  
<http://www.itaa.org/es>



1401 Wilson Boulevard, Suite 1100  
Arlington, Virginia 22209-2318  
PH: 703-522-5055  
FAX: 703-525-2279

**WARNING:** This message contains information that may be confidential and privileged. Unless you are the addressee (or authorized to receive for the addressee), you may not use, copy or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender and return the documents via U.S. mail.

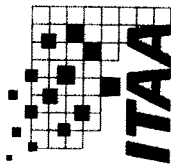
# Voting System Independent Testing and Certification Process:

Comprehensive, Rigorous, and Objective

Prepared by:

**The Election Technology Council**

November 2005



The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 350 corporate members throughout the U.S. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, ASP, digital content, systems integration, telecommunications, and enterprise solution fields. ITAA is secretary of the World Information Technology and Services Alliance, consisting of 67 IT trade associations around the world.

For more information visit [www.itaa.org](http://www.itaa.org).

## About The Election Technology Council

The Election Technology Council (ETC) is a group of companies that offer products and services which support the electoral process and have decided to work together to address common issues facing their industry. These companies believe that the voting infrastructure in the United States is in pressing need of improvement, and that electronic systems introduce new levels of voting inclusiveness, accuracy, efficiency, and accessibility. Working together as a division of the Information Technology Association of America (ITAA), ETC members will help election officials, lawmakers, voters, the media and others understand and better appreciate the benefits that technology can bring to the voting process.

Founding members of the ETC are: Advanced Voting Systems, Diebold Election Systems, Election Systems & Software, Hart InterCivic, Sequoia Voting Systems, and Unillect Corporation. The Council has been joined by Danaher Guardian Voting Systems, VoteHere, and Perfect Voting System.

The Council affirms its complete support for voting systems testing and certification. Trust in the American system of elections is of paramount importance to our members, as it is to all parties working in the elections community. Thorough testing and review in order to provide valid certification is an important component of that trust. Hence, the Council has resolved to offer its members' experience and insights on testing and certification to those parties undertaking a review of the certification process.

# Voting System Independent Testing & Certification Process:

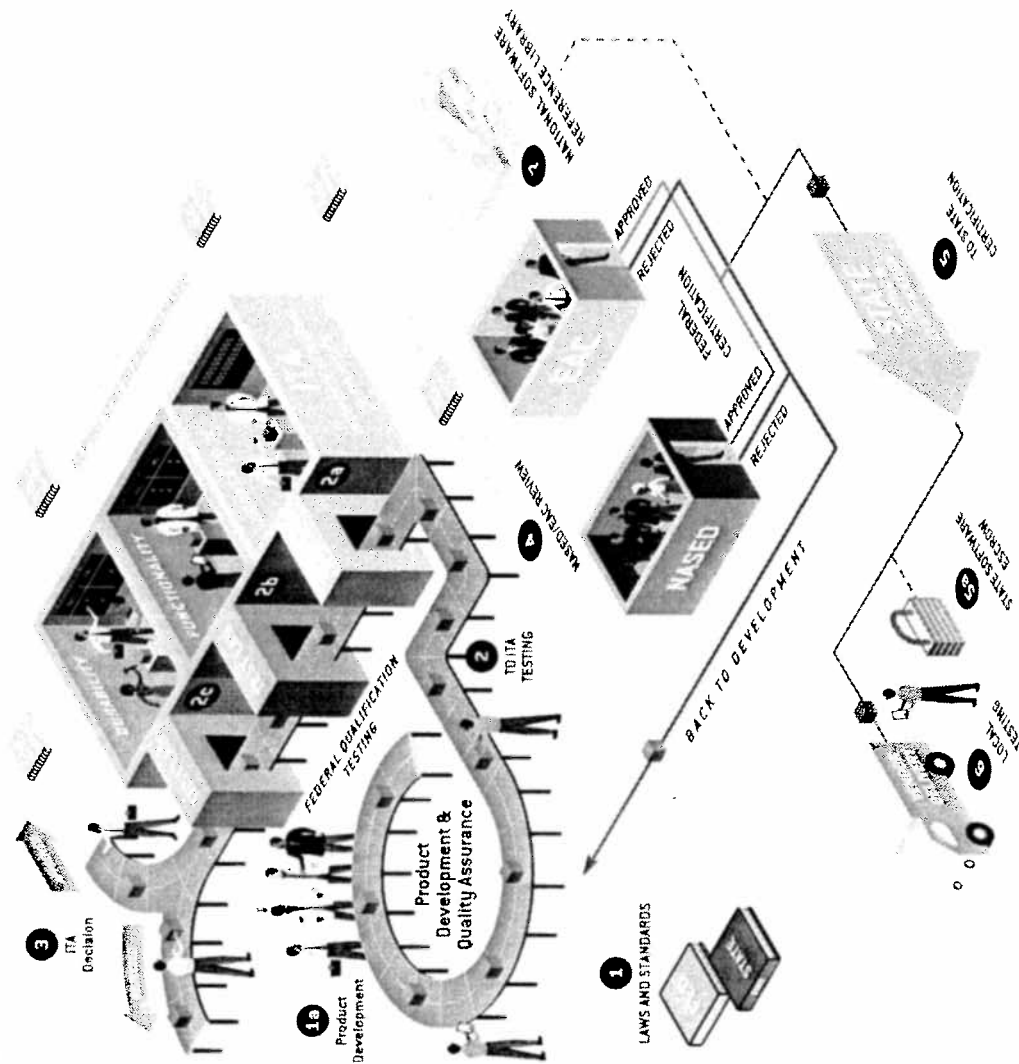
**Comprehensive, Rigorous, and Objective**

New and improved voting technology has made the election process easier, more accessible, and more secure.

These enhancements benefit election administrators and voters, and encourage participation in our

democracy. As technology has evolved, so, too, have procedures that ensure voting equipment deployed on Election Day is reliable, accurate, and secure. This overview depicts the

comprehensive, rigorous, and objective voting system testing and certification process - at the federal, state, and local levels.



**1. Standards Development:** Current and evolving state and federal law, regulations, and standards before requirements that must be met before voting equipment may be used in an election. Today, the Federal 2002 Voting Systems Standards provide guidance to vendors and the system testing bodies. New standards - the Voluntary Voting System Guidelines - are currently under development.

Election systems manufacturers continually conduct new product development to enhance current voting equipment and innovate the next generation of voting technology. This development process is driven by state and federal laws/standards that establish specific voting system requirements. It is also responsive to the needs of election administrators and voters.

**2. To IFA Testing:** After development, documentation, and quality assurance, to be certified to federal voting systems standards, a voting system and its component parts must go through extensive testing conducted by accredited independent testing laboratories (IFAs). This process begins with submission of a detailed Technical Data Packet (TDP) from the vendor.

IFAs review every line of software code to ensure compliance with standards and overall integrity. Once complete, an IFA will perform and witness the compilation of the source code into program-executable files.

IFAs test the functionality of the voting equipment using compiled code to ensure it operates accurately - that votes are properly captured, results are properly reported, and data is properly retained. To pass, a system must tabulate 1.5 million votes with 100% accuracy.

IFAs test the operation of the voting equipment to ensure it can withstand extreme environmental conditions and intensive human handling.

**3. IFA Reports:** If, at any point in the testing process, an IFA identifies an issue that must be addressed, a product or component part is sent back to the vendor for additional development and re-submission through the whole IFA testing process. Only after the system or component has passed every test is it deemed qualified for federal certification. An IFA compiles the results of the entire testing process into a report which is delivered to the EAC/NASED for further review.

**4. EAC/NASED Review:** The NAISED technical committee assesses the results of the IFA tests to ensure compliance with federal law and standards. If necessary, NAISED requests clarification from the IFA and/or additional development by the vendor. Only if a system passes this review does NAISED issue a number indicating formal federal certification of the specific version of the voting system.

**5. State Testing & Certification:** In a majority of states, federal certification is only a first step before a voting system can achieve state certification. In some cases, the state will carry out its own independent testing of the accuracy, security, and reliability of a system. State testing (which varies state to state) expands upon and enhances testing at the federal level. A state also will compare a product's features and functionality against state law and standards to ensure it complies.

Many states require the vendor to escrow a copy of the certified system software.

**6. Local Testing:** After production testing and upon delivery from a vendor, local election authorities conduct acceptance testing to ensure the voting system equipment performs properly and is certified. Further still, prior to voting elections, local authorities test the logic and accuracy of the equipment and procedures with election-specific ballots to confirm it functions properly and is secure.

**7. National Software Reference Library:** After software is federally certified, election system vendors can voluntarily submit the executable code to the National Software Reference Library, which archives a validation code for future reference. This allows jurisdictions to verify the delivered system software against the archived validation code to ensure it is the certified version.





757 North Broadway  
Milwaukee, Wisconsin 53202  
888.989.VOTE (8683)  
414.431.0180

**Testimony Against SB 296  
Provided by Anthony Boldin, President/Founder  
Voting Technologies International  
October 13, 2005**

Good morning, my name is Anthony Boldin and I am the President and Founder of Voting Technologies International, one of only a handful of voting system companies in the entire United States. We are very proud to be located right here in Wisconsin, and right in the heart of Downtown Milwaukee – well at least for now.

I am here in opposition of Senate Bill 296 because of four reasons – First, one of the authors has stated that this bill is necessary to meet HAVA - but Wisconsin law already meets Federal HAVA law requirements – no additional changes are required. Second, Wisconsin already requires a paper printout of each ballot cast at the time the ballot is cast, which makes this bill unnecessary. Third, it will not solve the security problems the authors intends it to solve. ...and fourth, it will essentially regulate us out of business in our home state.

After seeing the snafu caused by the dimpled chads in Florida, I knew there had to be a better way. With my knowledge of software and my desire to create a fraud-proof, affordable and easy to use voting system, I started my company, VTI, and have since invested millions of dollars into this company and it's employees.

Entrepreneurialism and innovation is what the Governor and the Senate has been working to enable here in Wisconsin for years. We are literally outraged about this bill - because the leadership of the state repeatedly states how they want to foster innovation and entrepreneurialism, yet when a company develops a system that solves the same problem that a piece of legislation intends to solve, it is almost completely disregarded. They want to legislate our Wisconsin-designed product out of existence and have it replaced by Ohio or Nebraska based companies. VTI is an innovative and entrepreneurial company – we need to keep companies like ours here in the state. Wisconsin should be begging for companies like ours, not putting them out of business.

The basic premise of the paper receipt is to give confidence to the voter. The confidence that their vote was cast as they intended, that there would be a

backup incase of lightning strike or some other disaster, or to facilitate a recount if needed. Indeed, we don't want to lose votes, we don't want unscrupulous people to change the vote (say to vote for one person and have it count for another), and we want to be able to have a fair recount, if necessary.

The newer high standards of the federal election commission (FEC) of 2002 requires voting systems to withstand all sorts of new electrical hazards. In fact, our system could be on a line that gets hit by lightning and it has been tested and proven to maintain it's high level of stability - no votes will be lost even in such an extreme circumstance.

The authors of this bill are well-intended, but they are not software designers. How would they know how to protect the public? Unfortunately, they just don't. We are and we've designed a system that does. Unfortunately, a paper printout is not a real defense against unscrupulous programmers, aka hackers, as this bill intends. A hacker that has the skill and desire to have a voting system record a vote for a person other than what you see on the screen will be just as able to have it record a vote for a person other than who was printed on the receipt. Yes, even though the Bill says "visually verifiable", no one can ever visually verify what is going on inside a computer. Even if the receipt is provided, it could record differently. False confidence is not the long term solution to having the electorate have trust and confidence in the voting process.

The only real way to assure that a voting system is guaranteed to vote for a person that you select on the screen, is not the paper receipt, but to assure that the software running on the machine is the one that is certified at the federal labs. Our system does just that - if the software running isn't the exact one certified at the labs, the system will not run and will require the user to reinstall the software so that it does match before launching the voting process. Without this verification, a paper receipt is almost worthless.

The only way to give the confidence that the vote was cast as intended is not to have a paper receipt, but to take an actual photograph of what they were looking at, at the exact time they cast their ballot. Our system takes this photo, or screenshot, of the screen with the voters choices, at the exact time their vote is cast. This photograph is then saved in multiple places and can be printed out or reviewed later in the case of a recount.

Therefore, the only real way to give true confidence to the voting public - that their vote will count as intended - is to give them a voting system that is safe, secure, and auditable - so that it can be trusted, not a feel good piece of paper. When we moved from pure paper to optical scanning many years ago, the change was just as scary, but the systems are trusted today. Over time through utilization the same will occur with electronic voting, the voting public will become comfortable with the technology after years of successful elections.

Additionally, there are many hidden financial costs of this bill. It is not only about 3-4000, \$100 printers and rolls of paper. It is really much greater than that. First, printers need to have paper changed, ink changed, and they jam up from time to time. Do we really expect our poll workers, who are mostly senior citizens, to have the skillsets of computer technicians? Or, maybe we are going to pay computer techs to man the polls now? Second, the speed that voters can be processed through a system with a paper receipt is slowed dramatically - about 20 percent slower than a system without. Why? Because voters are spending time reviewing their receipts and are also going to want to recast ballots in the case that they change their minds, even if there is nothing wrong. This means that the cost isn't just those \$100 printers anymore, it requires each voting location to have 20% more voting systems than they actually need. We're talking about at least \$2 million of unnecessary taxpayer expense here.

Lastly, we'd be reverting back to the old deficiencies of paper systems - they are all still there, but are now multiplied 10 fold. Why? Because receipts can be easily recreated by even a low-skilled individual. Depending on the system used, if paper receipts can be held by the voter, there could be fraud. There could then be ballot box stuffing by someone creating receipts that were never cast on a machine that would disrupt the recount process. But more importantly, there could also be vote buying, where voters keep their receipts in their pockets and put another piece of paper that looks like the receipt into the ballot box to make it appear as if they followed the proper procedure. This is the scariest one of all because it would be so easy to do.

Although the intention of this Bill is laudable, essentially wanting to bring security and confidence to the voting process, it unfortunately fails on many counts.

In summary, the only way to enable true voter confidence is to employ a voting system that can be trusted - such as the one that we have developed - which has already solved the problems that this Bill is trying to solve. Our system takes a photograph of the voters choices at the time the ballot is cast and our system validates that only state and federally certified software is running at the time of voting.

Unfortunately, the language of this bill would essentially assure non-approval of our system by the Elections Board, and would put us out of business here in Wisconsin and voting system companies from Ohio, Nebraska, or elsewhere would take our place.

For all of these reasons, we respectfully ask that you oppose Senate Bill 296 in it's current form. Lastly, I do have some written testimony for the committee to review. I hope that you would find some time to review them as well before making your final decision. Thank you very much for your attention here today. I would now be happy to answer any questions that you might have and then proceed with the demonstration.





no date

SB 276

## Voter Verifiable Paper Audit Trail... necessary or not?

This topic is one that is being discussed and decided upon by election officials in response to concerns raised by advocacy groups skeptical of the motives of some voting equipment suppliers and the accuracy of the systems they are selling. In an attempt to insure that elections be auditable, and to restore what they perceive as eroded voter confidence they are promoting that each voter be provided with a paper copy of each electronic vote. The theory being, that not only will the voter have a paper copy of his touch screen vote to verify if the computer registered his vote correctly, but this will also insure that there will be a paper trail for auditability purposes.

Unfortunately the paranoia being generated regarding touch screen voting equipment is based on incomplete information. The skeptics have chosen to completely ignore the regulated field process required to conduct an election, deciding rather to focus on lab conditions which are irrelevant. They have also based their platform on the evaluation of only a select few vendors products refusing to acknowledge systems that may satisfy their intent. Equally unfortunate is the additional costs that will befall the taxpayers because of this zealous effort to correct a process that may not need fixing.

To sooth the skeptics, many elected officials have opted to climb on the VVPAT bandwagon legislating expensive changes without completely evaluating all of the facts surrounding the claims being made. For those taking a more educated approach to understanding the validity and necessity for a voter verifiable receipt, Voting Technologies is providing the information in this document as an evaluation tool, to hopefully assist those making the decisions regarding VVPAT,

“There is no way to tell if the vote is accurate or not on a computerized voting machine, and because of this voter confidence has been eroded”. This is the battle cry of those who feel there is a giant conspiracy being perpetrated on the American voter to purposely rig elections in this county for political gain. Computer scientists and advocacy groups supported by a group of legislators, initiated VVPAT in an effort to restore what they perceived to be a lack voter confidence in new voting technology. They embarked on their cause, drew their conclusions and made generalizations on information that lacked investigative thoroughness. Because of this knee-jerk reaction and hysteria laden propaganda many election officials and legislators unfortunately bought into this unsupported logic, and mandated legislative reforms to provide voters with a paper receipt. For those are seeking to arrive at a more informed responsible decision we hope that the following questions will be addressed and answered during the evaluation process.

- 1) **Can the proponents of VVPT provide any documented evidence on any touch screen system that supports their claim that these systems can be hacked into, or tampered with to alter the outcome of an election?** There has never been a case of voter fraud, or equipment/ software tampering, with touch screen systems however there are numerous documented cases of fraud with paper based voting which is what they are advocating a return to. Touch

Screen systems are also not networked in any way contrary to claims being made.

- 2) **Why weren't all TS systems evaluated for their security and ability to be hacked into as these scientists who have contended is not only possible but likely to occur?** There are approximately 10-12 touch screen voting suppliers in the country today, yet the computer scientist only evaluated a couple of the larger companies to arrive at the generalized conclusion that all touch screen software is created equal. This is simply not true. Some systems utilize a Windows operating system and some use a Linux operating system, some use a Smart Card, others utilize Voter ID Pin numbers, some systems utilize older TS technology and some the more recent TS technology which makes calibration a non-issue. To lump all systems together merely reinforces the lack of thoroughness regarding the academia's claims.
- 3) **Is it really likely that any supplier would risk the legal consequences of tampering to affect the outcome of any election?** If voting equipment suppliers would have the capability to alter voting software to modify results or not count certain votes as the skeptics claim, then they surely could modify the software to adjust what the voter saw and what was printed out to achieve a desired result. Unfortunately the programming and coordination required to implement any modifications coupled with the severe legal penalties make this concern non-existent. To insure against tampering, Voting Technologies utilizes a series of checksums which insure that the certified software is the software which is being utilized for an election. In addition all of the activities that occur on each machine are logged by function and time, further guarding against any uninvited manipulation.
- 4) **What if the computer crashes or is hit by lightning and votes are lost?** This condition has been addressed in the most recent 2002 Federal testing standards and all certified voting systems have been tested for this type of failure. Should equipment malfunction or crash as skeptics have indicated all voting systems have multiple retrieval processes built into them. The Voting Technologies system has a UPS (Universal Power Supply), which is designed to protect the Election Processing Unit and hard drives against severe electrical and magnetic surges. VTI also provides multiple redundant backup of the votes cast to insure that no votes are lost including a paper copy, CD version and two (2) hard drives.
- 5) **Why do the skeptics fail to acknowledge the L & A testing that voting equipment is put through prior to every election to insure accuracy?** Because the skeptics do not understand the entire election process, they would rather ignore checks and balances if they don't support their cause. Pre-election testing is purposely designed to detect the inaccurate tabulation the

skeptics are contending is inherent in the software before the equipment is officially used to conduct an election.

- 6) **What is the audit/recount process of the various TS systems?** All TS systems have their own process of audit ability. The technology developed by VTI as an example, takes a photographic snap shot of each electronic ballot cast and stores it for future use. Each ballot picture can then be printed and hand counted for verification with the electronic vote if necessary.
  
- 7) **What are the proponents of VVPAT suggesting regarding the specifications of a voter receipt, and the implementation of their demands?** The answer is "very little". While insisting on a VVPAT for each voting booth, the skeptics have failed to define exactly what it is they want. They apparently feel the solution addressing the following consequential issues are better left to the very suppliers they vehemently distrust.
  - How large must the print be on the receipt to allow a visually impaired voter to verify his cast ballot? How large must the receipt be?
  - How will privacy be insured so another voter or poll worker would not be able to see a voters ballot receipt?
  - Can the voter take the receipt home with him? Does the printed ballot go behind glass? Into a box?
  - Does the receipt need to be printed in multiple languages?
  - How will the visually impaired voter receive a receipt?
  - What if voters are disenfranchised from voting because of long lines due to delays caused by voters verifying their ballot, jammed printers, and ink running out?
  - Does the receipt need to be printed before the ballot is cast or after it is cast?
  - If the ballot is printed after the voter casts the ballot and the voter claims that is not how they voted, what happens? Can the ballot be invalidated? How will this happen if voter confidentiality is to be maintained?
  
- 8) **Where is the proof that voter confidence has been eroded?** In study after study of voters who have used TS voting systems, they consistently rate their confidence in the ability of the new technology to record their vote properly at between 80% & 90%. In addition unlike in the past, today's voting equipment must pass stringent federal and state certification testing before it can ever be used in an election. This process has also served to strengthen voter confidence.
  - For the 10% - 20% of voters who do not have a confidence in electronic voting it would be a wiser and more fiscally responsible alternative to offer them the opportunity to vote on paper through an optical ballot since most counties utilize this type of voting in conjunction with TS as a means of accommodating absentee voting.

- 9) **Who will end up paying for the addition of printers for all of the touch screen machines in service?** The burden to fix a system that does not require fixing will ultimately befall the already burdened taxpayer. This is because Federal funding provided under HAVA will either be gone or insufficient enough to accommodate this modification. Here again the very suppliers that the skeptics distrust will gain financially from the insistence of this grass roots effort.

While the debate continues to forge on we can only hope that before any decisions are made resulting in long lasting implications, that all of the reasons for making any change are properly considered. For the officials responsible for evaluating the need for a voter verifiable paper receipt, we trust they will be prudent in their decision making process and seriously weigh the factors in determining a conclusion on this matter.