

Frequently Asked Questions Election Technology Council

What is the Election Technology Council?

The Election Technology Council (ETC) is a group of companies who 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, 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.

Who are the founding members?

Founding members of the ETC are: Advanced Voting Systems, Diebold Election Systems, Election Systems & Software, Hart InterCivic, Sequoia Voting Systems, and Unilect.

Is membership open to any electronic voting systems company?

Membership is open to any company in the election systems marketplace. To join ETC, companies must be or become members of the Information Technology Association of America (ITAA).

Why is the Council needed?

The Council has been established to help Americans understand and appreciate the benefits of electronic voting, and to assist those companies offering electronic voting solutions address a common set of business, technical and public policy issues. Council members have identified a number of programs to achieve these goals and established working groups to pursue them.

How is the Council connected to ITAA?

The Council is a committee in the Enterprise Solutions Division of ITAA. The Enterprise Solutions Division conducts programs focused on the government customer at the federal, state and local level.

Who is the chairman of the group?

The Council is chaired by David Hart, Chairman of Hart InterCivic.

What work will the Council perform?

The Council will focus its efforts in three general areas: technical, public outreach and advocacy. In the technology realm, the Council will address issues related to electronic voting system security, useability and certification. In terms of public outreach, the Council will conduct programs that help the public better understand the accuracy and reliability of electronic voting systems as well as the substantial collateral benefits, including ease of use and wider participation in the voting process. In addition to public education, the Council will reach out to government trade groups, community organizations, and interest groups involved in the voting process. In the legislative area, the Council will work to assure that the Help America Vote Act is fully funded at the state and local level.

How prevalent in the U.S. are DRE systems?

A survey by the International Foundation for Election Systems (IFES) finds that about 16 percent of election authorities are using DRE systems. Another 21 percent plan to convert to DRE systems in the future. By way of comparison, optical scanning technology is used by 34 percent of election authorities and 13 percent use lever action machines.¹

Why is electronic voting an improvement over older methods, such as punch cards, paper ballots or optical scanning?

Voting systems exist in a larger context—one characterized by people, processes and technology. Regardless of the technical solution, no device or system can offer assured performance if elections officials and polling staff are poorly trained, voting rules are not clearly defined, and related activities such as voter registration and records keeping are poorly conceived or executed.

With that in mind, the technology itself can make a major difference. The problems with punched card ballots were amply demonstrated and widely reported in the 2000 Presidential Election. Less well known, perhaps, is the fact that 2 million votes were lost to voting errors in each of the last four Presidential Elections.² Vote counting accuracy is the basic requirement for any voting system. But as these older voting methods demonstrate, even basic functionality remains a significant challenge. Beyond vote count accuracy, voting system technology has a role to play in areas like auditability, security, accessibility, participation (language minorities), ballot choice and configuration, voter confidentiality, and vote compilation (from sources such as absentee, mail-in and early voting).

While the characteristics of DRE systems vary, these voting solutions prevent voters from voting more than once (over voting) and provide mechanisms for allowing the voter

¹ <http://www.ifes.org/TechSurvey/data.html>

² Building Consensus on Election Reform, The Constitution Project, August 2001

to correct unintentional under voting. When balloting is completed, voting selections are presented back to the voter for verification so accuracy is far superior to punch card or optical scanner approaches. Systems generally provide options for the voter to go back and correct mistakes--again, a substantial improvement over older methods.

DRE systems offer accessibility features that assure both confidentiality and accessibility. The visually impaired, for instance, can use headphones to hear the ballot and cast a private vote, often for the first time.

Are electronic voting systems safe from tampering?

Electronic voting systems feature both physical and logical security at least as good and generally better than older forms of voting equipment. DRE systems do not feature keyboards or other peripherals that enable an infiltrator to tamper with software code or vote tabulations. Memory is locked in machines. Software code resident in voting machines passes through a series of checks performed by vendor personnel, certification professionals, government officials, multiparty observers and poll workers. The internal logic of source code, based on generic object identifiers rather than specific candidates, would make before the fact vote rigging difficult if not impossible. Systems may also store ballot definitions and other election data in redundant memory and verify this information after each vote. Discrepancies cause the system to shut down. Voting machines are not connected to the Internet, barring the possibility of over the network hacking. System access is protected by passwords, and the machines create extensive audit logs that document all system events, including malfunctions or tampering attempts. Taken together, the new generation voting system technologies provide greater security than current systems.

Can Internet hackers break into such systems and change results?

No. DRE systems do not connect to the Internet and so cannot be hacked.

Can voting cards be counterfeited allowing people to vote several times?

Manufacturers use digital signatures and other forms of encryption to make the chances of voting card counterfeiting remote. Other protections include the use of time, place, and election specific internal checks to assure card validity and to prevent cards from being used more than once.

Are you concerned that unscrupulous programmers will try to rig elections through deceptive software?

Of course--as we are with all possible risks no matter how remote. That concern has led to specific processes and policies to avoid such an event. For example, software code passes through numerous internal and external checks before use in an actual election, including rigorous certification testing by independent certification bodies. Voting system software is engineered months in advance of actual elections, making it very

unlikely for programmers to know who candidates will be and impossible to know how their names will appear on ballots. The source code is held in escrow by various state and federal officials, and local officials do not have access to it, thus preventing code changes at the local level.

Why not program voting systems with open source software so everyone can inspect code for potential vulnerabilities?

Open source software in an election context has benefits as well as problems. While the scrutiny of third parties may lead to the early identification and correction of vulnerabilities, it may also provide those intent on disrupting elections with a blueprint for understanding software design logic, knowledge of the business processes underlying elections, and the opportunity to introduce malicious code or apply “social engineering” techniques to perpetrate election fraud. Regardless, ETC members believe the proprietary versus open source issue must be decided by customers. If election administrators determine that open source software solutions are preferable, than vendors will offer open source software solutions. In any event, the source code is “open” to regulatory authorities at all times.

Should we have a national standard for voting system certification to which all vendors must submit their code to?

Voting system certification standards vary by state. ETC members believe that a single national standard would expedite the certification process. However, a federal standard would certainly raise issues of state sovereignty and would end up in the courts. The central issue is to create a process that is responsive to the changing demands of the customer and constantly evolving technology.

Shouldn't the public be concerned when uncertified machines wind up being used in elections?

ETC does not support having uncertified systems used in elections, but the use of uncertified voting machines in elections is an indication of a process breakdown, not a technology breakdown. In cases where this happens, the public should seek to satisfy itself that election officials have the situation appropriately identified and a corrective action plan in place.

Why not allow machines to print paper receipts for the sake of auditability and recounts?

ETC members do not advocate one way or another on paper receipts for each ballot cast. Rather, companies seek to provide products that meet customer requirements. The current generation of DREs supports this requirement. HAVA does not require that the paper ballot records be presented to the voter for confirmation of the ballot's accuracy. DRE systems present voters with the opportunity to verify vote accuracy on screen—an efficient, cost effective approach to assuring an accurate vote. However, most, if not all,

DRE systems have the technical capability to do so. The challenge is defining the laws, regulations, and processes that will be used to implement such a system, identifying and assessing the human factors that will affect how voters and poll workers use the system, and ensuring that implementation does not result in new problems and vulnerabilities that election officials, vendors, and advocates of paper ballots do not anticipate.

For example:

- Printing voter verifiable ballots adds several layers of cost and complexity to the process, accompanied by increased risk of failure at the polling place and the associated stress placed on poll works;
- Lines of voters may increase, as each voter takes additional time in the voting booth to reconsider his or her ballot; the resulting delays may disenfranchise some voters;
- Most DRE systems in operation today would need to be retrofitted to add the additional capability;
- Even the simplest issues must be thoroughly addressed. For instance, a lengthy set of ballot options would require a lengthy receipt for voters. Printers are likely to jam and run out of ink during election day operations, creating delays and dissatisfaction.
-

The time required to vote and verify a paper ballot will likely increase the amount of time a voter spends in a voting booth, requiring more voting systems and increasing costs. Further, voter verifiable paper receipts must consider the needs of blind and otherwise disabled voters in order to provide the same system attributes for all voters. In summary, when deciding this issue, government entities must weigh the difficult issues of implementation against the perceived benefits of a voter verifiable paper trail.

Without paper receipts, how do you do recounts should they be needed?

HAVA requires that voting systems have the internal capability of producing a hard copy tally of votes. DRE systems are capable of producing this record. This is a record intended for use by election officials in a recount situation, not a receipt for individual voters. Some systems also have the capability to produce results from multiple, independent data paths which can then be compared to identify data inconsistencies.

How often do electronic voting machines break down?

DRE systems are relatively new, generally in the marketplace for less than two years. As a result, statistics in this area are limited. Vendor reported experience with DRE break downs suggests that the rate is nominal. All vendors must submit their equipment to rigorous testing which includes tests to determine the ruggedness of the hardware. These tests assure that DREs can be expected to have a useful life well into the future.

Are unqualified vendors entering this marketplace?

With the federal government in the process of spending \$3.6 billion to upgrade state and local election technology, the prospect of many new entrants to the election systems marketplace seems likely. Because election law and process is complicated, with hundreds of jurisdictions and thousands of different ballot requirements, past experience and an in-depth understanding of issues in this domain is highly desirable. Many firms come into the DRE marketplace with a legacy of offering mechanical and optical election system products and services. Federal, state and local certification procedures provide another filter on market entry for unqualified vendors. Business reputation in a highly competitive marketplace is, perhaps, the ultimate safeguard.

Should the public be concerned about the “revolving door” of government election officials finding new jobs with election systems vendors?

Ethics laws for government officials in the election systems industry should be no less stringent than ethics laws for government officials moving to the private sector from other fields. Having said that, however, it would be both unfair and unrealistic to bar those with extensive knowledge and expertise in elections from pursuing a professional career in this area.

Who should I contact for more information about the ETC?

Michael Kerr
Director
ETC
703-284-5324
mkerr@itaa.org