# The Bell™

Privacy, Security and Technology in Internet Voting

NOVEMBER 2000 | Published Online Monthly | Vol. 1 No. 7

www.thebell.net | ISSN 1530-048X


*Mission bells were used in colonial California for telling time, announcing events, and for passing on news from one city to another. Our symbol is the classic outline of a mission bell because THE BELL newsletter serves similar purposes.*

## Web Page

Visit The Bell's web page at http://www.thebell.net – more information, more up-to-date.

## Call for Papers

Join the dialogue and submit your paper to THE BELL. See page 2. All papers are peer–reviewed. Submissions accepted at any time.

## Free Subscription

THE BELL is FREE of charge for Internet distribution in PDF format, and is also available in hard copy. For information, see the back cover.

# The Difference Between the Right and the Almost-right

*Editorial by Ed Gerck*

"The difference between the right word and the almost-right word is the difference between the lightning and the lightning-bug," said Mark Twain. The whole nation knows now that voting systems used in the U.S. are almost-right.

One requirement of a ballot-tallying system is that it should be possible, with a recount, to duplicate the result of an election. However, recounts are simply not exact with paper-based punch card and optical scan mark-sense ballots. Punch card systems may fail in 120,000 out of 6,000,000 votes. Optical scan ballots, in which voters indicate their choice by filling in ovals or squares, are sensitive to stray marks and may count them as a vote – for example, if a voter accidently pauses with a pen over an oval and then decides not to vote for any candidate. Either system may also count millions of false votes, since anyone can punch yet another chad or mark yet another oval in a blank vote even if overvoted ballots are automatically returned to voters.

How about electronic voting? DRE (Direct Recording Electronic) machines with touch screens have been around for more than 10 years in the U.S. and yet have only 9% of the market. The reason is that not only are DREs costly, but there is no clear reason to trust their vote count. DREs fail to prove that the counted vote is really what the voter voted. DREs are ideal "con machines" for voters – a DRE has no witness to its acts but itself.

Maybe now is the opportunity to do it right. Thirty-year-old Internet technology is coming of age. Internet voting can begin to be used in precincts, under current laws. It can cost $0.10 per vote. Let's put it through real-world tests and elections, with stronger requirements for voter privacy, vote secrecy, and election verifiability than current costly, error-prone, non-tamperproof, untrusted voting systems. Let's make every vote count, and count it right. The difference between the right voting system and the almost-right voting system is clear. One works, the other doesn't.

## Contents

**THE BELL™ Newsletter**
ISSN 1530-048X

**Editor:** Eva Waskell
editor@thebell.net

**Website:** www.thebell.net

**Address:** 1001 D Street, Suite 202, San Rafael, CA 94901-2800
**Phone:** (415) 482-9300
**Fax:** (415) 482-9400

**Privacy:** We will not forward to third parties any personal, address or credit information supplied to us by you. Any other information we may receive is treated as public and non-confidential.

**Submissions:** Contributions are welcome. Please see instructions at www.thebell.net/editor/.



# From the Editor

Dear Reader:

Hindsight is always 20/20. Sometimes, foresight also is. Six months ago, The Bell published an extensive national review of public voting in the states of Florida, California, Illinois, New York and Texas, prepared by Safevote. In this report, election officials talked openly about the unsolved difficulties with hanging chads and optical scan mark-sense ballots. The Bell wrote:

"The study revealed the tension in having the power to identify a problem while lacking the means to solve it. For example, for vote recounting the majority of paper punching systems used in the U.S. do not produce repeatable results when ballots are tallied more than once, which means that election officials lack the means to objectively distinguish between fraud and error under these circumstances. Thus, the timeliness and usefulness of this study to the election community, vendors and interest groups cannot be overstated, as well as its relevance toward future benchmarks to rate Internet voting systems. The study shows that the performance of current systems is not the 'golden benchmark' to which Internet voting systems should be compared. There are many faults with the current systems, as the report will describe, so we should in fact be looking to Internet voting systems in order to try to reduce those faults and thus provide for more security than what is available today –not less security."

Can Internet voting solve the accuracy and reliability problems that are a major factor in the drawn-out election in Florida? Possibly, but there's a danger that we may rush ahead too quickly and develop half-baked solutions, move toward unsafe systems, or simply bow to the pressure from those who believe that "something must be done" or that "this is a great market opportunity."

In this issue, Safevote proposes strict requirements for Internet voting, requirements which can be applied to all voting systems irrespective of the technology used. The IVTA tech Work Group has helped make the requirements more precise. Comments from individuals and other open Internet groups, such as Computer Professionals for Social Responsibility, were also incorporated. "When there are many eyes, all bugs are shallow," as I comment on the benefits of peer review in the article about certification and purchase of voting systems.

Eva Waskell
Editor

# Internet Voting Requirements

*by Safevote*[*]

*Safevote presents a proposal for strict Internet voting standards, with a set of 16 requirements that support fail-safe privacy, verifiable security and tamper-proof ballots. This set of requirements far exceeds the current requirements for paper-based ballots in the U.S., and also those for electronic voting DRE (Direct Recording Electronic) machines.*



## Introduction

This document provides a set of 16 strict requirements for Internet voting systems used in precinct-based voting. Precinct-based Internet voting provides direct training opportunities for all involved and is also a step toward eventually voting from one's home or office, as desired by the majority of Americans.

Having studied many alternatives, Safevote defined a basic architecture to ensure voter privacy, vote secrecy and election integrity within the scope of legal requirements for public elections, while providing for usability and low cost.

Since part of the system uses networks (dialup, Internet) to interconnect the parties involved and provide for oversight, there was a great concern about security and privacy. The distinguishing quality of the Internet is that no one can control both ends of a connection, neither sending nor receiving data. Opposite points may be under opposing controls. In particular, this makes it impossible to "measure" or authenticate the persons or processes at the remote end of an interaction, or even in-between, either sending or receiving. It is difficult to trust that which we cannot control.

However, ***the Internet can support reliable and secure transactions, and does so regularly, as long as all endpoints of the transactions are under the control of a single authority*** – even if multiple keys are used. People are generally unaware of this quality because it is not the "standard mode of operation" employed by the public in web browsing or sending an email.

Therefore, the reader is advised that as long as the endpoints fully control the cryptographic key agreement and node addressing schemes used, the "Internet as a transfer medium" is indeed extremely reliable in accurately delivering opaque blobs of encrypted and certified data, while Denial-of-Service (DoS) attacks can be forestalled by using the stealth, moving target technology described in http://www.safevote.com/tech.htm.

## 1. Precinct-based Internet Voting

This document focuses on the requirements for precinct-based Internet voting, where Internet voting stations are set up in polling places. This is very similar to Direct Recording Electronic (DRE) voting machines, but with a fraction of the cost while adding oversight and remote redundancy – functions that DREs do not have. A DRE operates alone, supervised only by itself and there is thus no clear reason to trust the vote count. DREs fail to prove that the counted vote is really what the voter voted. DREs are ideal "con machines" for voters –a DRE has no witness to its acts but itself. Lack of network connectivity is therefore not a positive factor for DREs, contrary to what one may think at first sight.

The benefits of precinct-based Internet voting systems following these requirements include 100% accuracy, large and clear ballot layout, tamper-proof ballots before and after casting the vote, physically redundant secure ballot copies, zero paper ballot costs, more voting places for the voter because the voter is not limited to voting at one precinct close to home, high reliability in terms of tabulating results, voter verification that his/her ballot is being counted, real-time auditing, effective human-verified recounting, and easy integration with state-wide or national tabulation. Some, but not all, of these benefits can be provided by current DRE voting machines. These benefits cannot be provided by paper-ballots, whether using punch cards or optical scan systems.

Even though the voting stations are not remotely located in precinct-based Internet voting, the use of digital certificates as a substitute for human-based control, "electronic ballots" in lieu of the traditional paper ballots, and remote ballot boxes in these requirements demand careful analysis. This document will first discuss the various components of an election system before presenting the requirements to provide the level of privacy and security mandated by public elections.

## 2. Remote Ballot Boxes

Voting systems comprise four main components: (1) a registration service for verifying and registering legitimate

voters; (2) voting stations where the voter makes choices on a ballot; (3) a device called the ballot box where the ballot is collected; and (4) a tallying service that counts the votes and announces the results. Additionally, voting systems have other components such as auditing, ballot generation, ballot management, recounting and storage.

Privacy, security and integrity of voting systems depend critically on these parts securely working together in combination, not just in isolation. However, these parts are not usually located at the same place and do not work together at the same time. The problem is to guarantee that their isolated actions do correspond to a system-wide policy, at all times and at all places, even though such actions may be remotely located to each other and done at different times.

**Central to this problem is the ballot itself.** Ballots need to be controlled from inception to end when they are generated, viewed, approved, controlled, distributed, voted, collected, tallied, audited, recounted and stored. Oftentimes ballots need to be defined per voter (e.g., when ballot rotation is used to reduce positional bias) or per class of voters (e.g., due to geo-political, regional and language differences). Also, law usually demands that whenever ballots are handled at least two election officials or authorized poll workers must be present. At the end of an election, law demands that all unused ballots must be accounted for. Various control procedures are used –e.g., with methods that provide only one-way access to the ballot box so that votes cannot be deleted or changed once they are cast. Further, ballots are usually confined within the physical limits of a poll site, under the supervision of poll workers. When transported to a tallying place, ballots are also physically protected.

Controlling the ballot is a well-defined task for paper ballots which can be physically designed as they will appear to a voter, physically printed, physically transported, physically counted and so on. The foregoing aspects may be protected by physical tamperproof seals, and may always involve the presence of at least two authorized officials. In order to compromise a paper ballot, several people need to be involved and collude in an entire mesh of events.

However, in Direct Recording Electronic (DRE) devices used in electronic voting, there is usually no paper to be printed and none to use for control. After the ballot is cast, a DRE may record anything as the ballot, not necessarily that which the voter voted. There are no unused ballots to be counted at the end of the election. The very definition of a "ballot" comes into question – what was the ballot image seen and used by the voter?

This problem is well-known in conventional systems for electronic voting. Virtually all DRE systems on the U.S. market have been certified according to the Federal Election Commission (FEC) Voting Systems Standards by accredited bodies. (For a complete list of certified systems, see www.electioncenter.org/about/nased.html). These standards define how ballot images are to be stored in such systems, and certified, before the elections. These standards are also specific about the storage of individual voter ballot images after voting, for example, as given in section 2.3.2 of the Standards, under "Accuracy and Integrity." However, in DREs there is no way of knowing whether that ballot image is really the ballot image seen and cast by the voter.

In conventional voting systems, whether paper-based or electronic, ballots may thus be provided by means of printed paper, non-volatile computer memory, CD-ROM, magnetic media, or any other way of storing and presenting the ballots, together with means to store the ballots cast until the votes are tallied. Conventional voting systems include several ways to protect the ballot and its voted contents from tampering or accidental errors.

However, dial-up and/or Internet networks can be used together with computers in order to define some aspects of ballot usage locally and also remotely, for example and as given in this document, by storing encrypted cast ballots at the local machine and also at servers which are not located at the poll site (and which might serve one or more poll sites). This may include local printing (at the precinct) and also remote printing, in paper, microfilm or other media.

Thus, in the case of electronic voting using the Internet or any other network (hereafter called network voting or Internet voting), ***the definition of an "electronic ballot" needs to consider electronic voting systems where the ballot boxes, the voting stations, the voter registration service, the tallying stations and/or any other component of the voting system may be remotely situated.***

Driving this evolution from paper-based voting to network voting are economic, political and social factors. For example, considerable cost reduction can be achieved by sharing costs in a client-server system with electronic data transfer, while providing increased voter participation due to greater availability of voting places for a voter, reduced physical transportation and physical security needs for transportation of ballot boxes, and reduced time for tabulating results.

Assuring the integrity of the election becomes difficult, however, when the ballot is handled remotely, outside the poll site. Locating ballot handling outside the poll site is at odds with the notion of protecting the ballot as conventionally done in poll sites. Locating the voting stations outside poll sites (remote voting) makes it difficult, for example, to verify whether the ballot is being correctly presented at the voter's home screen for example. Further, using the Internet for voting, voters may trivially and unavoidably change the window size where the ballot is displayed. Also, voters may independently change its colors, font size or other features. The operating system, which may vary from voter to voter in remote voting, may also display the ballot image differently than what was intended.

**(continued on p. 11)**

# Comments on Election System Management

*by Roy G. Saltman*[*]

*Ten years ago the author commented that in close contests "individual votes are important, and accurate counting of them equally so." But the solution requires accuracy, integrity, and reliability in the operational use of computer technology, and the capability to prove that these conditions are present.*

## Introduction

Computerized voting means either that voters employ computer-readable ballots and indicate their choices on the ballots with punched holes or pencil-made marks, or that voters make their selections directly on a specialized computer input unit, for example with push buttons. In either case, voters' choices are summarized by computing equipment, and a computer printout of the final counts is produced. Thus, computer-processed data is used as the basis of one of the most fundamental decisions of democracy: which persons are selected to govern.

There have been some administrative difficulties with computerized voting, and there has been a proportional lack of confidence in the specific results produced: in general, the greater the difficulties, the greater the lack of confidence. Concerns about computer use have been expressed by persons involved with the electoral process, as well as by journalists and computer-literate lay individuals concerned about the socially responsible use of these machines (Beiler, 1989a; Dugger, 1988; Elkins and Waskell, 1987; Nilsson, 1988; Trombley, 1989a, b, c) Examples of difficulties will be given. However, public confidence is not solely an issue of computer technology. Advancement of pure technology, hardware or software, may contribute, but will not suffice. The latest improvements in storage size, speed of operations, minimization of physical dimensions or power use, new computer languages, techniques of software design, or new intellectual concepts such as artificial intelligence, will not, by themselves, solve the essential concern.

The solution requires accuracy, integrity, and reliability in the operational use of computer technology, and the capability to prove that these conditions are present. This situation must occur in a particular area of public administration in which nearly every adult citizen has the right to be personally and directly involved. In addition, computer use in voting is part of a system involving people, established procedures, and activities, as well as equipment, and it is the entire system of those four elements for which public confidence is required.

## 1.1. Some Pertinent Events: Both Recent and Historical

A few days before the November 8, 1988 Presidential election, CBS Evening News included a segment about computerized voting. Anchorman Dan Rather interviewed both Howard J. Strauss, a computer scientist, and Penelope Bonsall of the Federal Election Commission (FEC).

Rather: "Voting in this country has gone increasingly high-tech with a potential, some experts warn, for high tech vote-count fraud. More and more Americans are voting by computer....Slick, 1980s technology ought to mean a high, very high, rate of reliability when it comes to tallying our votes. It ought to mean that, but it does not.

"Liste n to computer whiz Howard J. Strauss of Princeton. If somebody set out to break into the computer system, and actually alter the outcome of an election, its not only possible, but it's rather easy?"

Strauss: "The system has virtually no protection, no controls. It's not a house with doors without locks, its a house without doors."

Rather: "For the right kind of money, could you put the fix in, in a national election; realistically could it be done?"

Strauss: "Yes, get me employed by the company that writes this program. In that case, you only need bribe one person; one person writing the software for this company. You would have access to a third of the votes in the country. Is that enough to throw the election?"

Bonsall, director of the FEC's National Clearinghouse on Election Administration gave an opposing view:

Bonsall: "If you are talking about the ability or capability to compromise the Presidential election coming up on a wide-scale basis, I would say that that theoretical potential is close to nil."

What is the truth in this situation? Is the country in danger of massive vote-fraud due to compromised computer-tallying of voters' choices, or is that a fantasy of neo-Luddites disturbed by change to a modern technology? Even if nationwide elections are in no danger, how about local elections in which just one computer (not a nationwide set) need be manipulated? While it is important to know the facts about the level of election honesty, public perception of the facts may be, perhaps, even more important. Even if elections are honest, public perception that they are dishonest may be just as detrimental to the progress of democratic government.

Public confidence in the results is the major policy issue of computerized voting. This issue has been prominent ever since computerized voting began in the middle 1960s, and it remains the issue today. However, the question of public confidence has not been limited to computerized voting. This issue has always been important in our democratic form of government in which there are freely contested elections and in which final determination of winners is achieved by the popular vote of a massively enfranchised electorate. Election laws and administration have attempted to keep up with the technology of the times, but have not always been completely successful.

## 1.1.1 Historical Events

In 1934, Dr. Joseph P. Harris stated in Election Administration in the United States that:

"With the rise of large cities following the Civil War and the increase of immigration, election frauds became rampant.....As late as 1900, it was estimated by well informed observers that as many as 60,000 fraudulent votes were cast in hotly contested elections in Philadelphia...." (Harris, 1934, p. 18)

Election frauds were not confined to urban areas, despite Harris' implication in this quotation. Such frauds were, for example, part and parcel of the "county seat wars" fought in connection with the organizing of new counties in the Great Plains states in the last three decades of the 19th century. A recent article in Smithsonian, covering these disputes, discussed a county election held in Kansas in 1887. The article reported that an investigating commission had concluded that:

"This case can fairly be said to embody the sum of all election villainy. If there is any one particular crime connected with the conduct and the result of an election that was not committed in Gray county....we have failed to find it." (Chiles, 1990)

Dr. Harris also noted in his book that a counter trend began at the same time:

"A number of important trends in election laws appeared during the closing decades of the nineteenth century, brought on partly by the flagrant election frauds and violence which marked the conduct of elections throughout the country." (Harris, 1934, p. 19)

One important trend to which Harris referred was the introduction of lever machines after 1890. By the middle 1960s, it is likely that as many as 50% of U.S. voters made their selections on these machines.

## 1.1.2 A More Recent Controversy

A more recent election of interest is the presidential election contest of 1960, between John F. Kennedy and Richard M. Nixon. In this election, which occurred just a few years before computerized voting was introduced, there were serious charges of fraud in Chicago. Lever machines were in use throughout that city. One of the myths about this election is that (as stated recently in a California weekly newspaper):

"... Chicago's legendary Mayor Richard Daley,...historians believe, engineered President Kennedy's narrow margin of victory over Richard Nixon in the 1960 general election by stealing a key bloc of Illinois votes."

In this election, Kennedy received 303 electoral votes and Nixon received 219. Harry Byrd of Virginia received 15 electoral votes, including one from a faithless Oklahoma elector whose vote should have gone to Kennedy. Illinois' 27 electoral votes, if they had gone to Nixon, would have reduced Kennedy's total to 276, still more than a majority. In fact, if Nixon also had won Hawaii's 3 electoral votes, which Kennedy won by a mere 115 votes out of 185,000 cast, Kennedy still would have had more than the minimum requirement of 269 electoral votes. The California journalist needs to review the credentials of his referenced "historians."

The Chicago situation in the 1960 Presidential election has become the paradigm of mythical vote-stealing. Yet, there seems to be very little, if any, truth to the stories widely reported at the time. In fact, because of the furor, three distinguished University of Chicago political scientists authored an analysis of press coverage. They stated in their summary:

"What we have attempted to do is to examine the evidence put forward....to support the charges of fraud....On the basis of this analysis, we conclude that the charges that wholesale election fraud was perpetrated in Chicago were baseless and unsubstantiated." (Finer, Kerwin, and Pritchett, 1961, p. 3).

Their report also included the following: "A recheck of the voting machines in Chicago resulted in a net gain of 312 votes for Nixon out of a total of 1,780,000 votes cast--an amazingly accurate reporting of the vote....

**(continued on p. 14)**

# Certification and Purchase of Public Voting Systems

*By Eva Waskell*[*]

*The certification and purchase of election equipment for public voting systems, in the U.S. and around the world, is influenced by diverse cultural, social, political, and technical forces. However, it is possible to identify two main approaches in use, decentralization and centralization. The article also explains how open peer review, widely recognized as beneficial in the evolution of public Internet standards, is gaining ground in discussions of certification and purchase of public election equipment. The article highlights the fact that any technology used in elections has to be trusted by both election officials and voters if there is to be confidence in election results.*

## Introduction

There is a large variety in the manner in which election equipment is certified and purchased around the world. Social, cultural, political and technical considerations can impact the process at many different levels. In spite of this variety, it is possible to identify two main approaches in use today: a decentralized approach, as seen in the U.S., and a centralized approach, as seen in the majority of countries around the world.

A third approach to help certify and purchase voting systems can be seen in the open peer review process used widely to define Internet standards, most notably by the Internet Engineering Task Force (IETF). This process defines a standard not by a "top down" or even a "grass roots" approach but by the rather quantitative two-prong test of requiring "rough consensus and running code."

These are the fundamental building blocks of the method used by the Internet community to develop the protocols and standards used on the Internet. This is also the approach being used by the Internet Voting Technology Alliance (IVTA) for developing voluntary standards for Internet voting systems. It is a 30-year-old, time-tested and proven method that can successfully deal with the technical complexities of Internet voting and reasonably represent conflicting interests of vendors, developers, users and regulating bodies.

In addition, voters and election officials are likely to have more confidence in an open peer review process, as opposed to the current proprietary voting systems which implement security through obscurity and subject the purchasers of their systems to the "trust me treatment."

It would be useful to understand these different approaches in order to better appreciate the impact each one has on the administration of the election process, including the voting process, and ultimately on the voters themselves.

## 1. A Decentralized System

The decentralization of the certification and purchase of election equipment in the U.S. is an outgrowth of the decentralization of election administration as a whole.

The origins of this process can be found in Article I, Section 4 of the U.S. Constitution which states: "The times, places, and manner of holding elections for Senators and Representatives shall be prescribed in each State by the Legislature thereof; but Congress may at any time by law make or alter such Regulations, except as to the Places of chusing Senators."

Thus, each individual state has exercised its right to administer elections in a manner reflecting that state's political, social and cultural make-up. Although the Constitution clearly gives Congress the authority to make or alter such state regulations, Congress has been very reluctant to do so. However, Congress *has* intervened in state election procedures when, for example, they gave women the right to vote and when they passed the Voting Rights Act. Nonetheless, states' rights have taken precedence when it comes to conducting elections.

When voting systems are certified by a state, they may have to meet the standards drawn up by the Federal Election Commission (FEC). While the FEC voting system standards of 1990 are voluntary, many states have adopted them as the minimum requirement for the certification of voting systems. States also may have additional requirements of their own, a state board of voting system examiners or private consultants who inspect the voting systems and issue their own reports regarding the suitability of a particular system for that state. Florida has the "gold standard" of voting system certification. Their specifications exceed the FEC standards and the certification process is known throughout the election industry to be very thorough (and very time-consuming). On the other hand, some states have adopted the FEC standards as the only requirement for voting systems. In short, each state has its own method and criteria for certifying voting equipment.

In the past, voting equipment vendors had to go to each state, one at a time, to certify their systems before they could be used in that state. But the use of Independent Testing Authorities (ITAs) is turning an expensive and time-consuming process into something more streamlined and centralized. It works as follows. Vendors take their systems to an ITA to certify that they meet the FEC standards. The ITA then files a report with The Election Center (www.electioncenter.org) or it may send the report directly to a state election director. In the case of Florida, the report is forwarded to the Florida Voting System Section. Wyle Labs does the hardware evaluation and Nichols Research does the software evaluation. Both ITAs are located in Huntsville, Alabama.

The National Association of State Election Directors (NASED) (http://www.nased.org) has played a central role in making this project a reality. NASED works closely with the ITAs and The Election Center which acts as secretariat for the NASED ITA Committee. The Houston-based Election Center keeps copies of the certification reports from the ITAs and maintains a website listing the specific make and models of voting systems that have earned ITA certification. All states, including those that do not have the resources to design, develop and conduct their own certification process, will benefit from this project.

Once a voting system is certified by a state, the counties, cities, townships or other subdivisions are free to decide which certified system to purchase and use in their elections. Nevada and Louisiana are two exceptions. In these cases, it is the state election department that purchases equipment and gives it to the respective counties/parishes.

It is important to distinguish between several types of testing in this area. The qualification testing done by the ITAs "implies conformance with standards and functional requirements, and may be done once to satisfy many States. Certification ensures that the product meets State requirements. Acceptance testing evaluates the degree to which the specific units delivered to the local government conform to approved characteristics." [Roy G. Saltman, Accuracy, Integrity, and Security in Computerized Vote-Tallying, NBS Special Publication 500-158, August 1988, page 3.] The entire testing process for proprietary voting systems is relatively closed and confined to a rather small number of individuals when compared to the thousands of people from around the world involved in the open testing process for protocols or software used on the Internet. However, this relatively closed process may involve *more* individuals than those in the centralized system described below.

## 2. A Centralized System

In a centralized or top-down system, there is one federal office that certifies and authorizes the purchase of all election equipment, even though the actual purchase may be decentralized.

The federal office strictly follows the procedures outlined in law. It does not make or interpret any election rules; it only does what the law allows. Input to this office usually includes a board of advisors and representatives of political parties. The vendors of election equipment sell directly to the federal office. Federal control is exerted by determining what voting system shall be used nationwide or by defining the regional budget for the purchase of approved voting systems. Once the equipment has been purchased, the federal office is responsible for distributing it to the various regions of the country. The regional centers in turn distribute the equipment directly to the local poll sites.

This is only one example of how a federally controlled system might work. For a comprehensive overview of worldwide election administration and extensive details about specific countries, visit the website of The Administration and Cost of Elections Project (www.aceproject.org) This website is an electronic encyclopedia of election administration developed in conjunction with the United Nations and the International Institute for Democracy and Electoral Assistance. Another useful resource is the International Foundation for Election Systems (www.ifes.org) which collects and disseminates election-related information and materials.

## 3. An Open Peer Review System

The Internet has been a very successful mixture of technology and business. Many believe that the major reason for this success is that Internet protocols were designed and developed using an open peer review process using the two-prong test of "rough consensus and running code" in order to define what works and what does not.

In other words, getting the technology right is not only what matters. Technology *and* social impact are the deciding factors behind the building blocks of the Internet.

Before becoming a standard for writing software for hardware used on the Internet, a protocol needs to meet two conditions: (1) rough consensus among the technical experts and users regarding its design, and (2) software based on such a protocol has to run reasonably without problems or surprises (even though it may have known bugs or deficiencies).

In order to get to the stage of "running code," sufficient testing of the protocol *and* software is necessary to discover any bugs and improve where necessary. These tests are conducted in an open environment and watched very closely by technical experts. Test results are made public and widely circulated. Thus, it is very hard to hide something that is not working as it should. In short, before there is "running code," there is lots and lots of open and public testing.

**(continued on p. 14)**

# Contra Costa Internet Voting Test

*Edited by Thomas Blood*[*]

*The author works with Safevote as Security Architect. This article presents a collection of public references relevant to the Contra Costa Internet Voting Test performed by Safevote under contract with the California Secretary of State, from October 30th to November 3rd. Only references which are available online are included.*

**1. Voters Get a Peek at the Future: Computer Ballot Demonstrations Set**

A few hundred, perhaps thousands, of voters in Contra Costa, San Diego, San Mateo and Sacramento counties will be among the first to vote in a certified presidential election via the Internet this fall. While their votes won't actually count, officials say fulfilling one's civic duty from the comfort of a home computer is merely a matter of time. ``It's more than just a matter of security,'' said Steve Weir, head of Contra Costa County's elections department. ``The first issue we have to grapple with is the secrecy of the voter. Second is authenticating that the voter is who they say they are. Third is building a security system that's hacker-proof.''
http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/10/09/MN49233.DTL

**2. Cyberspace Voting Wins Approval: Online ballot 'coming,' election official says**

"In the Bay Area and throughout California, we're ready to accept online voting,'' said Steve Weir, head of Contra Costa County's elections department. "It's going to come slower than the consumer wants, but it's coming. No doubt about that.'' Of 539 people surveyed, 82 percent indicated that they would vote online if given the opportunity, according to a report released in October 2000 by Active Research, a Burlingame, California company. Of those asked, 63 percent said they would vote in more elections if they could do so on the Internet. Only 15 percent said they would continue to cast their ballots by conventional means.
http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/11/07/MN44700.DTL

**3. Hackers Invited to Muck Up Mock Ballot**

Calling all hackers: A California company testing the possibility of online voting wants hackers to try to break into its system. The idea is to test whether online voting would be secure, says Alfie Charles of the secretary of state's office. The results will help the state determine the risk of tampering before moving from paper to pixels. While three companies and four counties are participating in the test, only Safevote, of San Rafael, is inviting hackers to test its system, even giving necessary addresses to help them "get closer to our inner circle of defense," CEO Ed Gerck says. The company also is setting up a phone hotline and e-mail address for questions; answers will be posted online. "What we are asking is to help us understand our limits," he said.
http://www.usatoday.com/life/cyber/tech/jk110200.htm

**4. A Vote for Online Ballots**

All paper limitations of ballots, from language barriers to confining voters to the polling stations closest to their home, disappear when voting moves online. "This system would totally prevent accuracy problems. We can put a much more accurate ballot on the screen than they can put on paper, says Ed Gerck, CEO of San Rafael (Calif.) online-voting systems company Safevote.
http://www.businessweek.com/bwdaily/dnflash/nov2000/nf20001115_536.htm

**5. Ballots Need an Upgrade – Duh!**

According to Ed Gerck, the CEO of the electronic voting firm Safevote, Florida alone shouldn't be pilloried. He said that Palm Beach-type chaos occurs all the time with punch card voting systems–we just don't see it because the vote count usually isn't close enough to make a difference. States use paper ballots because of "inertia," he said. They're what election officials know best, they're what voters know best, and because of that–because we haven't known anything else–they've become sacred in American democracy.
http://www.wired.com/news/politics/0,1283,40078,00.html

**6. Safevote Invites Hackers To Give It A Crack**

Safevote Inc. is testing its Internet voting system in Contra Costa County this week. As part of the preparations for live elections online in Californian precincts, the company is asking Internet users to attempt break-ins. To make it easier for hackers the company has posted various information online, including network configuration, details about all secret keys, and a range of computer IP addresses. "This information would be relatively easy for attackers to obtain," said Ed Gerck, chief executive officer of Safevote. "This is a test designed to expose any weaknesses the system may have. We want attackers to get as close as possible to the inner circles of defense, circles which must not fail."
http://www.newsbytes.com/news/00/157447.html
http://www.iactual.com/noticias.cfm?GUID=4322
http://www.telekomnet.com/news/10-31-00_safevote_hackers.asp

http://biz.yahoo.com/bw/001030/ca_safevot.html
http://www.net-security.org/text/press/972959801,71516,.shtml

**7. Internet Voting Shows Promise During a Trial Run in Martinez**
In an op-ed piece, Ed Gerck of Safevote explains that elections bring a special security challenge: a "privacy wall" is needed between the i-voter and the electronic ballot. The security technology used in e-commerce cannot even be considered. No one but election officials must control the entire Internet voting process. Openness must approach the absolute: All computer programs and protocols must be open for public review, so that any citizen can see that there is nothing to hide. Electronic ballots must be verifiable but never identify the voter, even under court order. Election integrity needs fail-safe assurances.
http://www.sacbee.com/voices/news/voices05_20001121.html

**8. Marin Firm Touts Software for Safe Voting via the Net**
Ed Gerck has studied the shortcomings of paper balloting for the past four years and commissioned a study earlier this year of 18 counties in five states, including Broward County in Florida where Democrats have requested a hand count. "If the election is close, that is when you need accuracy. That's when the system matters and it doesn't work when it matters most," Gerck said.
http://www.marinij.com/news/stories/news4001538.shtml

**9. CBS MarketWatch Interview with Ed Gerck**
This is the second interview by CBS MarketWatch with Ed Gerck, following up on Internet voting. This interview covers details of the attack challenge issued in the Internet voting test in Contra Costa County, California. Gerck also talks about the unreliability and accuracy problems with current paper-based voting systems and explains how Internet voting can raise the bar for election privacy, security, accuracy and integrity.
http://www2.marketwatch.com/video/default.asp?clip=1108safe

**10. Florida Electronic Elections**
Events in Florida are causing people to look closely at Internet voting. Conscious of the importance of the questions raised, Safevote, a company in the area of San Francisco, under contract with the State of California - conducted a test of Internet voting parallel to the true electoral process. The company invited hackers to try to penetrate the election system and provided information necessary to assist in the attack. Apparently, nobody was successful. The test was done with machines installed in place of the traditional ballot boxes. The company said that the test is "a step toward the possibility of voting at home or office."
http://www.lemonde.fr/aietek/edition/mobiles/article/0,3629,116499-2861-3005,00.html

**11. Florida Shows the Need to Modernize the Election Process**
An interview with Ed Gerck, CEO of Safevote, Inc., highlights the problems with paper-based voting systems and points out the advantages of Internet voting.
http://www.oglobo.com.br/mundo/12MUN401.htm

**12. Test of Cybervotes in Silicon Valley**
Four counties in California will test Internet voting in the November 2000 Presidential election in a partnership with the California secretary of state.
http://194.185.98.154/online/tecnologie_internet/votoviaweb/sanmateo/sanmateo.html

**13. Four California Counties to Test Voting via the Internet**
This month, San Mateo and three other counties will launch the first online voting projects in the state. They're out to test the latest technology and the concept that the click of a mouse is the key to a more democratic future.
http://www.sjmercury.com/svtech/news/front/docs/vote100300.htm

**14. Computer Voting System Built by the Clueless**
Safevote is obviously intimately familiar with the literature on voting schemes. Their 'Information Center' lists many of the most important papers published on this topic in recent years, and many patents. Just because you don't have a clue whether the patents are valid doesn't make them clueless. In any case, invalid patents usually are 'worth something', as they are cheap to create and expensive to destroy. Nevertheless I would advise Safevote to waive their patent rights. This would make the DVC and other techniques appealing to other individuals and organisations, leading to more interest and more serious attacks, and greatly increasing its prospects. A 30% share, say, of a large market is worth much more than a monopoly on something no-one uses. It's a shame you ignored all the interesting aspects of the trial. As far as I know, this is the first implementation of a modern voting scheme. It uses homomorphic encryption, so you can add the votes together before decrypting the total: you never ever decrypt an individual vote.
http://www.technocrat.net/973229523

Thomas Blood has degrees from the California State University at Monterey Bay, Monterey, CA, Master of Arts (2000) in Information Management and International Security Affairs, and the World College West, Petaluma, CA, Bachelor of Arts (1992). Blood was with the U.S. Army from 1990 to 1997 as an Intelligence Analyst, involved with signals intelligence analysis and the elaboration of intelligence briefs. In 1999 he was Classified Lab Manager of the Defense Manpower Data Center (DMDC), Monterey, CA, where from 1997 to 1999 he also provided data extracts and analysis in support of the Office of the Secretary of Defense, the Pentagon, and Congress. Thomas Blood is the Security Architect at Safevote. He can be reached at tblood@safevote.com

# Internet Voting Requirements

**(continued from p. 4)**

Other aspects that come into play when ballots are handled outside controlled environments are, for example: to protect the identity of the voter, to prevent the voter from voting twice, to prevent attacks that might deny access to a remote ballot box or from a remote voting station, to assure vote secrecy and voter privacy, to provide for auditing and vote recounting. Automation and networking also increase the possibility of widespread fraud, viruses, Trojan horses, hacker attacks, or simple bugs in software which can unfairly bias the results of an election. Both vote accuracy as well as reliability may sharply decrease when either one or both the ballot box and the voting station are located outside the same poll site.

Thus, several difficulties arise to potentially undermine the integrity of elections in network voting, many of which are posed by questions related to the very definition of a ballot and how it is controlled. Methods used in conventional systems to assure integrity of elections by physically controlling the number and style of ballots, whether in paper or provided by a machine at the poll site, cannot be applied. Unsupervised handling of ballots is also unavoidable. Viruses and Trojan horses, for example, may easily change what a voter sees on a screen in spite of the correct information being sent by a central server that dispenses valid ballots, or in spite of what a voter may type on the keyboard, even when using an encrypted communication channel between the machine used by the voter and the server.

## 3. The Wallet Approach And Verifiability

In conventional systems, one solution to this problem is the "wallet" approach used in e-commerce. This solution can be recognized in some Internet voting systems undergoing public tests. In this type of solution, a communications system is defined in which a particular Object (a "control structure," for example, a Java applet or a browser plug-in –also called a "wallet" in e-commerce protocols such as SET) is installed or transferred from a server (ballot server) to a client (voting station). That control structure is a special piece of software which encapsulates ***both*** (1) data fully defining the intended server-client communications relationship, including the ballot; and (2) methods for using the data to effect that relationship, including reading and verifying a voter's digital certificate, displaying the ballot, reading the voter's choices and casting the ballot. After it is transferred to the client, the Object as a control structure runs on the client side to control communications between client and server. According to this solution, once the client computer receives such an Object, it needs only to access the Object's methods. The Object handles all communications details including cryptographic or other modules, which modules may be embedded in the Object itself or referenced by means of digital signatures to certified modules outside the Object.

The problems with the "wallet" approach are well-known in the art in e-commerce and include, for example: long downloads of hundreds of kilobytes or even some megabytes of data; unreliable behavior because the client stations may not adequately support the resources required by the "wallet" (e.g., memory, browser version); the need for frequent version changes due to bugs or discovered attacks leading to a repeated need to download ever newer versions of the "wallet" (with all the time, certification and cost penalties involved); the need to rely on the user to install the "wallet" without interruptions even in the event of varying access speed; and heavy traffic load on the "wallet" server. In fact, the shortcomings are so severe that the "wallet" approach has already been abandoned in e-commerce.

In voting, there are further shortcomings to the "wallet" approach. Contrary to e-commerce, voting demands anonymity. Also, voting cannot be protected by insurance against fraud such that a certain level of fraud can be accepted as "the cost of doing business." Thus, there must be official verification and public trust that the "wallet" does not include malicious code or covert channels that would either bias the vote or reveal the voter's identity – which verification and trust are time consuming to achieve and yet must be repeated for each new version of the "wallet." Possibly, this process will actually incur growing distrust as problems are discovered, as has been experienced in e-commerce applications of similar technology.

Also, Trojan horses or computer viruses at the client side may easily subvert the "control structure" and render useless all efforts to control the ballot, how it is presented and how it is voted. Again, in e-commerce this may be compensated by insurance, which is not the case in network voting.

Further, although the order of candidates may be rotated and/or incremented in the ballot to prevent bias, anyone who sees the first ballot and gets access to the source code, to the downloaded binary image or to the file image of the code will be in a position to learn the assignment table between candidates and accumulators that carry the vote, in total or in part. Thus, a virus or Trojan horse attack could be designed even with ballot rotation and could be used to bias the outcome of the election.

These forms of attack become greatly facilitated when the source code is open (as oftentimes and herein required for security purposes), when the system uses the Internet for any of its parts, when the software is available for study in compiled form in electronic voting machines or servers used for demonstrations prior to the election, when the attacker may gain access to the software by any means, or when the election extends over several days – as many as

twenty-nine days of voting are being considered for Internet voting, for example.

Another problem in conventional voting systems, especially important in network voting, is to provide for verifiability, i.e. to be able to verify whether a particular voter voted – but without revealing how or when that voter voted.

Verifiability may be performed by auditors (in auditing) or by anyone including the voters themselves in what is called "universal verifiability." Methods that provide for verifiability while an election is in progress are useful to help deter fraud, minimize costs after a fraud is discovered, contain a discovered fraud, and even allow an election to proceed normally after a fraud attempt is discovered. However, methods that provide for verifiability usually rely on a listing of the voter's real name, which is not only ambiguous (i.e., for common voter names such as "John Smith") but also introduces the question whether that voter's name does correspond to one and only one vote. Still other methods try to solve the question of identical voter names by assigning "voter codes" to each voter, which raises the question whether such assignment has not been compromised by a hacker attack or unwittingly, by a "bug".

Another flawed method is one that lists the voters' real names (or linked voter codes) together with their respective encrypted ballots and intends to provide voter anonymity by tallying the ballots without decrypting them (called homomorphic encryption). But even if the encryption is perfectly secure, such method cannot protect voter privacy in the case of a court order that would ask to decrypt the ballots one by one. This method's privacy assurance relies on one weak link – that individual ballot encryption will never be broken. Besides a court order, unauthorized decryption (e.g., by an attacker, by collusion, by design faults, by lost or stolen passwords) or unintended decryption (e.g., using an area in memory as the accumulator, which area is watched for increments as each vote is tallied, by a virus or Trojan horse) is hard to prevent and impossible to disprove in conventional systems, especially because voted ballot information needs to be kept for a long time (due to legal, auditing and recounting needs).

## 4. Voting Protocols

Other types of cryptographic voting protocols have been proposed, the suitability of each type varying with the conditions under which it is to be applied. However, the questions introduced by remote ballot boxes and *electronic ballot* management, which need to be handled both *before* voting (e.g., ballot certification, ballot distribution to voters, ballot style authentication) and *after* voting (e.g., auditing of tallied ballots, auditing of ballot images), are not discussed in such protocols – which protocols are thus useful only for a limited theoretical discussion of voting, without a more comprehensive theoretical modeling or even a practical network voting system in mind. These voting protocols include schemes using mix-nets, homomorphic encryption, and blind signatures.

Clearly, for electronic voting on networks where the ballot box and/or the voting stations are remotely situated these issues need to be revisited with a fresh perspective. It is not possible to neglect problems facing remote ballot control.

## 5. The Multifold System

What is needed first is to change paradigms and avoid the "Fort Knox Syndrome" model exemplified by the dictum "make it stronger!" so widely seen in conventional security designs, including the "wallet" design. The "Fort Knox Syndrome" model fails to solve the problem of how to provide secure network voting because in this model the entire chain can still be compromised by failure of one weak link – even if that link is made stronger. And the addition of any link, even if very strong, would not make the system less vulnerable, and might make the system more vulnerable because the security of the system would still depend on the weakest link (which might be the newest link). Further, such solutions are actually based on ***the impossible assumption that "no part will fail at any time"*** –because if a critical part fails, the system fails.

As used in this specification, the solution followed by Safevote (U.S. patents pending 60/225996, 60/226042, 60/226158, 60/231600, 60/231681 and others) uses multiple links arranged in time and space, which links build a special multifold of closed control loops (***a meshwork***) under the principle that every action needs both a trusted introducer and a trusted witness, thus building two open-ended trust chains for every action. ***These closed control loops allow trusted properties in the system to always rely on self-trust, which is the only trust that is always verifiable.*** By making the issuer of a *Digital Vote Certificate* (*DVC*, see http://www.safevote.com/aboutus.htm) also become the final verifier of the same *DVC*, an off-line end-to-end security system can be built that is always verifiable. ***This closes the "loop of trust" and forces all endpoints of the transactions to be under the control of a single authority (who may use split keys) – the election officials (see Introduction).***

Further, by introducing suitable redundancy and information-theoretic "one-way walls," one can use these principles to design systems that can be as secure as desired. For example, one can design a ***collusion-free system*** by adding enough parts so that even if M parts fail at the same time (e.g., all key-holders collude), the system will still provide the expected functionality. One can also design a ***fail-safe system*** where M parts can fail at any time, even if M is the entire number of parts.

In terms of risk models, the closed-loop multifold link system used by Safevote (U.S. patent pending, as above) implements a multi-risk design – exemplified in this document with a simple equation in first order analysis:

**A = B * C**

where A = average amount lost, B = probability of failure and C = value at stake.

***Clearly, one can equally well call "risk" either A or B or C.*** Each choice leads, however, to a different risk model. If risk = A, this means that one is talking about the security of the system as a whole, for a certain period of time, in terms of average loss. If risk = B this means that one is talking about an individual transaction in terms of probability of loss of one event for a significant ensemble of events. If risk = C this means that one is talking about risk as total loss over a period of time long enough so that one can observe repeated failure events until losses have eroded all that was at stake (being nothing else left, the loss ends there, hence the risk).

In the closed loop multifold link system used by Safevote, the risk model that considers risk = C is called "fail-safe" for any risk beyond C, because C is all there is ever to be lost in the system even if every link fails.

Thus, rather than seeking "infinite protection" by one link (which is clearly impossible and mitigates against the "wallet" solution), a secure network voting system could provide for a measure of protection as large as desired by using an open-ended, closed loop multifold of links, each link individually affording some "finite" protection and collectively contributing to higher-orders of integrity in closed loops of trust.

## 6. Requirements

An Internet voting system needs thus to satisfy various requirements, which are summarized in 16 main points (examples can be found in the references given at the end):

1. ***Fail-safe voter privacy.*** Define: "voter privacy is the inability to know who the voter is." Assure voter privacy even if everything fails and everyone colludes.
2. ***Collusion-free vote secrecy.*** Define: "vote secrecy is the inability to know what the vote is." Assure vote secrecy even if all ballots are made public and everyone who holds decryption keys collude.
3. ***Verifiable election integrity.*** Define: "election integrity is the inability of any number of parties to influence the outcome of an election except by properly voting." Assure universal verifiability of election integrity, including voter verifiability directly at the remote ballot box.
4. ***Fail-safe privacy in universal verifiability.*** If the encrypted ballots are successfully attacked, even with court order, the voter's name must not be revealed. In addition, the system must provide for "information-theoretic privacy" (i.e., privacy which cannot be broken by computation, even with unbounded time and resources) in contrast to systems that would only provide for "computational privacy" (i.e., privacy which could be broken by computation, given time and resources).
5. ***Physical recounting and auditing.*** Provide properties for auditing and vote recounting, which are particularly difficult to trust in network voting, by means of multiple channels for closed-loop timestamp, authentication and non-repudiation proofs that can be physically stored, recalled and compared off-line and in real-time during the election, without compromising election integrity or voter privacy, and allowing effective human verification.
6. ***100% accuracy.*** Every vote or absence of vote (blank vote) must be correctly counted, with zero error.
7. ***Represent blank votes.*** Allow voters to change choices from 'vote' to 'blank vote' and vice-versa, at will, for any race and number of times, before casting the ballot.
8. ***Prevent overvotes.*** Warn the voter that a vote has to be cleared before making another choice in multiple vote lists, as needed. This warning should be made known only to the voter, without public disclosure.
9. ***Provide for null ballots.*** As may be required by law, allow voters to null races or even the entire ballot as an option (e.g., to counter coercion; to protest against lack of voting options).
10. ***Allow undervotes.*** If it is desired that the voter receives a warning of undervoting, this warning should neither be public nor prevent undervoting.
11. ***Authenticated ballot styles.*** Ballot style and ballot rotation to be used by each voter must be authenticated and must be provided without any other control structure but that given by the voter authentication process itself.
12. ***Meshwork of links.*** Use a multifold of links *and* keys to securely define, authenticate and control "*electronic ballots*" suitable for voting with remote ballot boxes, while forestalling Denial-of-Service (DoS) attacks (see Introduction). Provide levels of access, privacy, security and integrity comparable or better than conventional voting systems, even though remote ballot boxes and/or remote voting stations may be used.
13. ***Off-line secure control structure.*** Provide for an off-line secure end-to-end control structure for the *electronic ballots*, by means of digital certificates under a single authority (such as *DVCs*, see Section 5 and Introduction). *Electronic ballot* control must also be data-independent, representation-independent and language-independent.
14. ***Technology independent.*** Enable *electronic ballots* and their control to be used off-line and/or in dial-up and/or in networks such as the Internet, with standard PCs or hand-held devices used to implement their components in hardware or in software, alone or in combination for each part.
15. ***Authenticated user-defined presentation.*** Enable such an *electronic ballot* system to dynamically support multiple languages, font sizes and layouts, so that voters could choose the language and display format they would be most comfortable with when voting, as allowed by law and as may be required by voters with disabilities, without any compromise or change to the overall system, from an authenticated list of choices.
16. ***Open review, open code.*** Allow all source code to be publicly known and verified (open source code, open peer review). The availability and security of the system must not rely on keeping its code or rules secret (which cannot be guaranteed), or in limiting access to only a few people (who may collude or commit a confidence breach voluntarily or involuntarily), or in preventing an attacker from observing any number of ballots and protocol messages (i.e., the system must have zero-knowledge properties). Only keys may be considered secret.

According to the specifications herein and restricted to controlled voting stations in precinct-based Internet voting, such a system can be built today, providing for DoS protection, voter anonymity, vote secrecy and election integrity in Internet voting, as exemplified in tests conducted by Safevote –such as the public test in Contra Costa County reported on page 9 of this issue.

These requirements were edited by Ed Gerck, including comments and references from Tony Bartoletti, Thomas Blood, Elaine Maurer, Roy Saltman, Einar Stefferud, Eva Waskell, the IVTA tech WG (http://www.mail-archive.com/tech@ivta.org/), Safevote's website and previous articles in The Bell.

# Comments on Election System Management

**(continued from p. 6)**

"The State Electoral Board, composed of four Republicans and one Democrat, certified the Kennedy victory in the state on the ground that there was not sufficient evidence of fraud in Cook County (which includes Chicago) to change the canvass." (Finer, Kerwin, and Pritchett, 1961, pp. 10, 11)

In the Nixon-Kennedy race, there were many very close state-wide contests, in addition to Hawaii. Kennedy won Illinois by less than 9000 votes out of 2.7 million cast. Nixon won California by 35,000 out of 6.5 million cast. Kennedy also won close contests in Michigan, Minnesota, Missouri, Nevada, New Jersey, and South Carolina, as Nixon did in Alaska. The closeness of these contests shows that individual votes are important, and accurate counting of them equally so.

Later, in the era of computerized voting, there would be other stories of vote-count disputes. In these situations, the inability of election administrators to manage the new technology would be seen to play a major role.

**Continues in the next issue: Election Administration.**

Roy G. Saltman, M.S., M.P.A., works as a consultant in computerized voting. He is retired from the U.S. National Institute of Standards and Technology (NIST) and is well-known for his reports and presentations on the integrity of computerized voting. He is a member of the Advisory Board of the Internet Voting Technology Alliance (IVTA). Saltman can be contacted by email at roysalt@aol.com, by phone at (410) 730-4983 or by fax at (410) 997-4355.

# Certification and Purchase of Public Voting Systems

**(continued from p. 8)**

What about rough consensus? Where and how is it formed? Consensus regarding the design/test work takes place in open, online technical work groups. These online work groups also evaluate the testing procedures, scrutinize the test results closely, and finally reach rough consensus on whether or not a proposed protocol can become a standard. And, as often said in open peer review groups, "When there are many eyes, all bugs are shallow." This approach has served the Internet community (and the general public) very well. It is a time-tested method and one that has been proven to work. ***It is essential that this established tradition of openness, peer review, rough consensus and running code be maintained in the design and development of Internet voting standards.***

How would an open peer review approach work in support of certification and purchase of voting systems worldwide? The first thing to point out is that an open peer review system focused on Internet voting would coexist and interact with other peer review standard-setting organizations (like the IETF) as well as with current decentralized and centralized systems of certifying and purchasing election equipment. Such coexistence means that each country can maintain its independence in administering elections –as it rightly should –and at the same time have the benefit of technology that has been verified by the broadest possible input of experts, users and voters. *One of the unique advantages of a truly open system is that voters can have a permanent peer review forum where their input can directly influence the design and even choice of a voting system.*

## The Internet Voting Technology Alliance

One such forum is the Internet Voting Technology Alliance (IVTA), at http://www.ivta.org, an open peer review body dedicated to serving the public by acting as an information center, discussion forum, voluntary standards setting body and web publisher focused on Internet voting. The charter for the IVTA tech Work Group is at http://www.ivta.org/tech/charter/txt) WGs are open to anyone. All messages are archived for anyone to read. This degree of openness ensures both public scrutiny at every step and the widest possible technical input and evaluation.

Hence, purchasers of voting systems and voters may use open peer review to avoid the "trust me treatment," especially when it comes to integrity, privacy and security assurances.

Eva Waskell has been involved with the U.S. election system and computerized elections since 1985. She has a background in software programming. Her research regarding election-related lawsuits became the primary source material for a July 1985 New York Times article on the vulnerability of computerized voting systems. She is the Communications Director of Safevote, editor of The Bell newsletter and a member of the Advisory Board of the Internet Voting Technology Alliance (IVTA). She can be reached at ewaskell@safevote.com

# Media Watch & Links

**NVA, Compaq and Cisco Systems Announce $10M Investment in VoteHere.net**
The funds will be used to certify and deploy VoteHere.net's online voting application as the company enters what is expected to be the biggest growth year for the adoption and purchase of online voting systems.
http://www.votehere.net

**PoliticsOnline: Is Online Voting the Solution?**
This is a large collection of links to publications in the wake of the current drawn-out election.
http://www.politicsonline.com/pol2000/onlinevotereconn.asp

**The Case for Electronic Voting**
Bill Taylor, a vice president of Internet voting firm election.com, said his company is moving full-steam-ahead with remote voting, and they will not develop electronic voting terminals for precincts.
http://www.wired.com/news/politics/0,1283,40141,00.html

**Hack the Vote**
... in an era where home and office computer users continue to fall prey to viruses and worms, it's harder to ensure that a vote hasn't been changed by a program that has secret control of the voter's machine.
http://www.securityfocus.com/templates/article.html?id=114

**Online Voting, Even if Secure, Won't Solve Election Troubles**
Some experts think the problems of last week [Florida] could be solved by computerized voting, while others insist that it's fraught with insecurity.
http://www.latimes.com/business/columns/techcol/todays.topstory.htm

**Dan Gillmor: U.S. Election Process is in Desperate Need of an Upgrade**
We don't need to create a new monopoly here by settling on a single kind of machine. Rather, to promote competition, we should create a standardized platform, if you will, that vendors could bid on to provide to individual localities.
http://www0.mercurycenter.com/svtech/news/indepth/docs/dg111000.htm

**Online Voting Still Meets Resistance**
Despite the high-profile debut of Internet voting in March, election chiefs worried about its reliability will restrict its use this Election Day.
http://www.usatoday.com/life/cyber/tech/cti727.htm

**Time to Digitize Elections**
http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/11/27/BU91491.DTL

# From Our Readers

**From Hugh Denton, Assistant County Registrar, Contra Costa County, CA**
"I used the Safevote system myself and I liked it. It was very easy to use. Overall I can say that the test in our county was successful and the reaction from the people who voted on the system was very favorable. Many voters I talked to wanted to know when they would be able to use it for real, including voting from their homes or offices. I think Internet voting can also be used at the precinct, allowing voters to cast their ballots anywhere in the county. Voting was reasonably fast and could have been even faster if there were more than one computer issuing DVCs. My staff members also found the system easy to use and operate."

**From Christina Constantikes, Director of Email Sales, Sigaba Corporation**
"The Bell is excellent. It looks at difficult situations head-on. It's very concise and focused. My work involves Internet security and I find it a valuable resource."

**From Jackie Gloger, President, Melbourne Technical Services, Inc.**
"It's a fantastic newsletter. Very educational. And there's so much different information covered. It helps us to keep in tune with what's happening out there and to understand all of the changes that are going to be coming our way."

**From Norma Lyons, Elections Supervisor, Gwinnett County, GA**
"Internet voting on a large scale basis is many years away from being practical and secure. The Federal Election Commission does not support the idea of Internet voting nor does the Public Integrity Unit of the United States Justice Department. In any event, until it is permitted by law in Georgia it won't be reality here."

**From Dr. Richard Shurtz, host of the "Tech Talk" show on WMAL Radio in Washington, DC.**
..."The Bell, a newsletter that I have enjoyed reading up to the October issue. ... when will the November issue of Bell be out?"

**THE BELL™ Newsletter on Internet Voting**

**THE BELL c/o Safevote, Inc.**
**1001 D Street, Suite 202**
**San Rafael, CA 94901-2800**

**FIRST-CLASS MAIL**
**U.S. POSTAGE PAID**
**SAN RAFAEL, CA**
**PERMIT NO. 896**

**DATED MATERIAL**
**Please Expedite**

**FIRST-CLASS MAIL**

# Internet Voting Requirements See p. 3

**To enter your FREE monthly subscription, visit the website www.thebell.net or use the form below.**

**cut here** **M A I L O R D E R F O R M** **cut here**

**Enter your one year monthly subscription to THE BELL: visit the website www.thebell.net or fill out the form below**

**Privacy Notice: We will not forward to third parties any personal, address or credit information supplied to us by you.**

**NAME/TITLE**_____

**COMPANY**_____

**ADDRESS**_____

**E-MAIL**_____

**[ ] PDF 12-Month Subscription – FREE**

**[ ] Printed 12-Month Subscription – $ 30.00 SUBJECT TO AVAILABILITY**

**[ ] Year 2000 Public Sector U.S. Market Intelligence Study, 200+ pages – $ 850.00 SUBJECT TO AVAILABILITY**

**[ ] Hard-copy Six Issues of THE BELL, 96 pages, from May to October/2000 - $ 15.00 SUBJECT TO AVAILABILITY**

**INSTRUCTIONS: Mail completed order form to the address below. Pay by CHECK or MONEY ORDER, payable to Safevote, Inc. Allow two weeks for processing.**

**THE BELL c/o Safevote, Inc.**
**1001 D Street, Suite 202 San Rafael, CA 94901-2800**