California Secretary of State Bill Jones

California Internet Voting Task Force

A Report on the Feasibility of Internet Voting
January, 2000

Bill Jones
Secretary of State
1500 11th Street
Sacramento, California
www.ss.ca.gov

Internet Voting Report

Executive Summary

The California Internet Voting Task Force was convened by Secretary of State Bill Jones to study the feasibility of using the Internet to conduct elections in California. More than two dozen experts in the field of data security, elections and voter participation were asked to volunteer their time and expertise in the development of this report. The recommendations, analysis and suggested technical requirements that follow represent the collective opinion of the task force.

Opinion of the Task Force

The implementation of Internet voting would allow increased access to the voting process for millions of potential voters who do not regularly participate in our elections. However, technological threats to the security, integrity and secrecy of Internet ballots are significant. The possibility of "Virus" and "Trojan Horse" software attacks on home and office computers used for voting is very real and, although they are preventable, could result in a number of problems ranging from a denial of service to the submission of electronically altered ballots.

Despite these challenges, it is technologically possible to utilize the Internet to develop an additional method of voting that would be at least as secure from vote-tampering as the current absentee ballot process in California. At this time, it would not be legally, practically or fiscally feasible to develop a comprehensive remote Internet voting system that would completely replace the current paper process used for voter registration, voting, and the collection of initiative, referendum and recall petition signatures.

To achieve the goal of providing voters with the opportunity to cast their ballots at any time from any place via the Internet, this task force believes that the elections process would be best served by a strategy of evolutionary rather than revolutionary change. This report defines four distinct Internet voting models and the corresponding technical and design requirements that must be met when implementing any of the stages.

One of the most difficult tasks for an Internet voting system is the authentication of voters. To ensure that every voter has the opportunity to cast a ballot and no voter is able to vote more than one time, this task force believes election officials should initially test Internet Voting technology through the use of Internet Voting machines that are under the direct control of election personnel in traditional polling places.

Eventually, election officials can transition toward allowing voters to cast ballots at publicly accessible county-controlled kiosks or computers and, in the future, provide the option of remote computer voting from any computer with Internet access.

If remote Internet voting is eventually adopted, this task force believes that current technology requires that it initially be modeled on the current absentee ballot process in California. Although the procedures used to request an Internet ballot in this model would be more cumbersome than traditional e-commerce transactions, it is the only way to tie the authentication of voters from the existing paper voter registration system to the electronic arena at this time.

We believe that additional technical innovations are necessary before remote Internet voting can be widely implemented as a useful tool to improve participation in the elections process in California. However, current technology would allow for the implementation of new voting systems that would allow voters to cast a ballot over the Internet from a computer at any one of a number of county-controlled polling places in a county.

As with most computer systems, increased security and higher levels of privacy can be provided by increasing the complexity and the burden on the user of the system. The success or failure of Internet voting in the near-term may well depend on the ability of computer programmers and election officials to design a system where the burden of the additional duties placed on voters does not outweigh the benefits derived from the increased flexibility provided by the Internet voting system.

The democratic process warrants an extremely high level of security, but the security measures can not be so cumbersome to voters that the new process would prevent participation. An appropriate balance between security, accessibility and ease of use must be achieved before Internet voting systems should be deployed.

Major Findings and Recommendations

Definitions of Internet Voting

- For the purposes of this report, an *Internet Voting System* is defined as an election system that uses electronic ballots that would allow voters to transmit their voted ballot to election officials over the Internet.

- *Internet Voting* means the casting of a secure and secret electronic ballot that is transmitted to election officials using the Internet.

- An *Internet Voting Machine* is defined as the computer hardware that allows an electronic ballot to be cast over the Internet.

- *Polling Place Internet Voting* is defined as the use of Internet Voting Machines at traditional polling places staffed by election officials who assist in the authentication of voters before ballots are cast.

- *Remote Internet Voting* means the unsupervised use of an Internet Voting Machine to cast a ballot over the Internet using a computer not necessarily owned and operated by election personnel. Authentication of the voter would rely on procedures outlined later in this report, but must include some form of identity verification that is at least as secure as existing voting procedures.

Evolution of Internet Voting

- The implementation of Internet Voting will be a complex undertaking with no room for error. This task force recommends a phased-in approach to developing an Internet Voting System that will allow election officials and voters the opportunity to identify any possible problems before they occur.

- Phase One of the task force's recommendation would provide for the use of Internet Voting technology in a supervised setting like a traditional polling place. In this phase, voters would not yet gain the advantage of voting from any place at any time, but the integrity of the voting and tabulation technology will be verified through the use of Internet Voting Machines.

- Phase Two of the task force's recommendation would allow voters to cast Remote Internet Ballots. The authentication of voter identity would take place with a combination of manual and electronic procedures that would provide at least the same level of security as the existing voting process.

Internet Voting Process

- For the foreseeable future, Internet Voting should be viewed only as a supplement to, not a replacement of, traditional paper-based voting.

- The design of any Internet voting system must be at least as secure against fraud as the current absentee ballot process in every respect.

- All election activities stem from voter registration which is a paper-based system maintained locally by 58 county election offices. Until digital signatures and digital identification are a common aspect of everyday life for all Californians, on-line registration and the eventual collection of on-line petition signatures for initiative, referendum and recall campaigns should not be made available.

- Until the voter registration rolls contain a digital signature or biometric identification for all registered voters, requests for Remote Internet ballots must

be made on paper with a manual signature that can be compared against the manual signature on the voter's registration card. Voters will be provided a digital signature for voting purposes once the manual signature on the Internet ballot request and the paper voter registration card are verified.

- Internet voting systems must be designed to protect the secrecy of the ballot, while providing election officials with an audit trail that can be used to conduct recounts of election results.

Technical Issues

- Potential criminal electronic attacks on computer software, such as destructive "viruses" or "Trojan Horse" software, create a serious threat to Internet voting. To minimize the potential technological threats to Internet voting, election officials should provide unique operating system and web browser software to voters.

- To achieve the required level of security for a remote Internet ballot, voters will be required to take several precautionary steps before voting. For remote Internet voting to be successful, the burden of the additional duties placed on voters must not outweigh the benefits to be derived from the increased flexibility provided by an Internet voting system.

- Ballot integrity and secrecy can be protected while ballots are transmitted over the Internet through the use of digital signature and encryption technology. All identifying information used to electronically verify the identity of a voter shall be stripped from the ballot prior to the tabulation of the votes to ensure the secrecy of all Internet ballots.

- Although the voter's ballot will be protected from alteration or infringement of privacy as it travels over the Internet, the ballots of voters who access the Internet through a local area network may have their privacy breached by a network administrator who can access the voter's computer while the ballot is in an unencrypted state. To prevent a breach of privacy, voters must be warned of this potential problem and substantial penalties must be imposed on network administrators who attempt to violate a voter's privacy.

State and Federal Election Laws

- Several state and federal laws mandate equal access to the voting process and restrict state and local authority regarding the implementation of new election laws. Care must be taken to ensure that Internet voting applications are accessible to all voters.

- Internet Voting opportunities must be accessible to all voters, including low income voters whose only access to the Internet may be through public access Internet terminals that are commonly available in libraries and schools.

- Internet ballots must be available in multiple languages in jurisdictions required to print multi-language ballots to conform to the Federal Voting Rights Act.

Impact on County Election Officials

- County election officials would require significant fiscal and human resources to undertake the implementation of either polling place or remote Internet Voting Systems.

- Just as county officials are currently required to ensure each voter's paper ballot is configured properly, they would have the additional burden of simultaneously ensuring proper ballot configuration on the electronic system.

- County officials would need to ensure that their paper and Internet voting systems are properly integrated to ensure proper tabulation of ballots from both systems.

- Voters will receive the information they need to cast and encrypt their Internet ballot from county election officials. County officials will be responsible for comparing signatures on Internet ballot request forms with each voter's signature on their voter registration card. If the signature on the ballot request form is verified, the county would then be responsible for providing the voter with an electronic identifier that will be used for authentication over the Internet.

- Counties will need trained technical personnel to assist with the implementation of Internet Voting Systems for each election.

Public Acceptance

- Recent public opinion polls show that support for Internet Voting is strongest among those members of the public who have the greatest access to and familiarity with the Internet. Younger voters and voters in the western region of the United States have a higher degree of Internet proficiency and a higher degree of support for Internet Voting at this time.

- The plausibility and popularity of Internet voting is likely to rise over time as public access to and use of the Internet approaches the levels of home telephone and television usage.

- The level of public support for Internet voting must be measured in terms of all potential voters, not just the universe of voters who are likely to utilize this form of voting. If Internet voting is viewed skeptically by a large number of voters, then the fundamental trust in the democratic process may be compromised.

Task Force Composition

In pursuit of additional tools that might help improve participation in and the administration of elections, California Secretary of State Bill Jones convened the following panel of experts to study the feasibility of Internet Voting. The Task Force was asked to report on the legal and technical challenges that might be encountered in the implementation of a system that would allow voters to cast ballots over the Internet.

The chairman of the Task Force was Alfred Charles, Assistant Secretary of State for eGovernment. David Jefferson, Systems Engineer for Compaq Computers, was appointed to serve as Chair of the Technical Issues Committee. And Linda Valenty, Assistant Professor of Political Science at San Jose State University was appointed to Chair the Practical Issues Committee.

Regular Task Force Members

Alfie Charles
Task Force Chair
Secretary of State
Sacramento, CA

David Jefferson
Technology Chair
Compaq Computers
Palo Alto, CA

Linda O. Valenty, PhD
Policy Issues Chair
Assistant Professor of Political Science
San Jose State University

Jim Adler
VoteHere.Net
Kirkland, WA

Pete Adlerberg
VoteHere.Net
Kirkland, WA

Sylvia Ahern
Sterling Software
Redwood City, CA

Kim Alexander
California Voter Foundation
Sacramento, CA

Michael Alvarez
California Institute of Technology
Pasadena, CA

Dwight Beattie
Sacramento County Elections
Sacramento, CA

Kaye Caldwell
Silicon Valley Software Industry
Coalition
Capitola, CA

Jacquie Canfield
League of Women Voters
Fresno CA

Assemblyman Jim Cunneen
State Capitol
Sacramento, CA

Steve Cunningham
Cisco Systems
San Jose, CA

Roger Dao
County of Santa Clara
San Jose, CA

Tim Draper
Draper, Fisher, Jurvetson
Redwood City, CA

Brian Gangler
Secretary of State
Sacramento, CA

Pam Giarrizzo
Secretary of State
Sacramento, CA

Mikel Haas
San Diego County Registrar of Voters
San Diego, CA

Tom Hill
Secretary of State
Sacramento, CA

Thad Howard
The Howard Agency
Sacramento, CA

Steve Knecht
Global Election Systems
Novato, CA

Rom Lopez
Assembly Elections Committee
Sacramento, CA

Stacey Morgan
Assemblyman Jim Cunneen
Campbell, CA

John Mott-Smith
Secretary of State
Sacramento, CA

Philip Muller
President
Political Technologies, Inc.
San Francisco, CA

Jonathan Nagler
UC Riverside
Riverside, CA

Cameron O'Rourke
Oracle
Rocklin, CA

Mark Reynolds
iLumin Corporation
Orem, UT

Joe Rodota
Executive Producer
FAQvoter.com
San Jose, CA

Peter Schmidt
Cisco Systems
San Jose, CA

Warren Slocum
San Mateo County
Assessor/Clerk/Recorder
Redwood City, CA

Larry Sokol
Senate Elections Committee
Sacramento, CA

Bernard Soriano
Secretary of State
Sacramento, CA

James L. Wayman
National Biometric Test Center
San Jose, CA

Introduction

What is Internet Voting

For the purposes of this report, the term "Internet Voting" is used to describe a voting process that would enable voters to cast a secure and secret ballot over the Internet.

Under the phased-in implementation approach recommended by this task force, voters could use the Internet to cast ballots initially from a traditional polling place, but eventually they would be able to vote electronically from a remote location, such as a public Internet Voting kiosk or the voter's home or office.

While implementation of Polling Place Internet Voting would be similar in many ways to the implementation of existing electronic voting systems, the implementation of Remote Internet Voting would require numerous technical and procedural innovations to ensure accurate voter authentication, ballot secrecy and security.

Until all potential voters have access to a unique form of electronic identification, election officials will be unable to develop a digital voter roll that eventually could be used to authenticate voters for voting purposes, allow Internet voter registration or digitally sign petitions for use in the initiative, referendum and recall process.

In light of these shortcoming (and others) that prevent a total replacement of the current paper-based voting systems, this task force recommends that Internet Voting Systems should strive to provide an *additional* method of voting that would give voters increased opportunities to cast their ballot. The task force has used the California absentee ballot as a model for the design of a Remote Internet Ballot.

We recommend that any use of the Internet for voting purposes should be phased-in gradually to ensure that election officials and members of the public are confident in the technology.

Brief History of Voting Systems

The American election process has been evolving since its inception. The right to vote has been revised and extended by four constitutional amendments and several judicial and legislative actions. The voting process itself has been subjected to near constant change over the last two hundred years.

Early American elections were conducted by such rudimentary methods as a show of hands and the depositing of beans and/or grain into a box to indicate voter preference. For much of the 19th century, ballots were printed and *pre-marked* by political parties. The voter was essentially just a conduit for the straight ticket voting demands of the party.

In 1888, the first "Australian Secret Ballot" was adopted in Massachusetts. The "Australian Ballot" is an official ballot printed at public expense on which the names of all nominated candidates appear. It is distributed only at the polling place and voted in secret. California adopted the "Australian Ballot" in 1891.

Since that time, numerous other revisions to the voting process have taken place, the most recent of which include the adoption of postcard mail-in voter registration, vote-by-mail absentee ballots and the recent approval of computerized touch-screen voting systems.

Election Equipment

Early voting machines were used to ensure accuracy of the count and prevent election official errors and official misconduct. Thomas Edison invented the first election machine in 1869. Since that time, various voting systems have been approved, implemented, revised and rejected.

The predominant voting technology implemented by county election offices today is the use of punch cards. Long ballots and the logistical complexities of moving thousands of machines to polling places for each election prompted counties to switch from large voting machines to the smaller, more flexible punch-card systems.

To help improve the voting experience and reduce the cost associated with printing paper ballot cards, electronic voting systems have recently been approved and are now being deployed in various voting jurisdictions.

With the proliferation of new technology designed to improve efficiency in virtually every aspect of daily life, members of the voting public and political scientists are now focussing on ways to make the voting process more accessible and substantially less complex for both the voter and the election official.

By simplifying the election process and providing increased access to voting locations, we should be able to draw more people into the democratic process.

Approval of Election Equipment

In California, county officials conduct the day-to-day functions of the election process. The Secretary of State is the Chief Elections Officer and is charged with general oversight of the California Elections Code.

The Secretary of State is responsible for maintaining a "List of Approved Election Systems" that counties must consult prior to purchasing and implementing election hardware and software. Currently, nine different election systems are used by various counties throughout the state – ranging from optical scanning systems to punch cards.

Electronic voting systems, including systems that utilize touch-screen technology, have also been approved and have recently been implemented on a limited basis in select counties.

Approval of Internet Voting Systems

The use of the Internet for voting in official state and local government-sanctioned elections in California could be implemented in some instances with the certification of an election system by the Secretary of State. For the more advanced stages of remote Internet voting, three stages of government approval may be required: 1) The State Legislature would have to amend the elections code to adapt the current paper-ballot voting requirements to the electronic voting and vote tabulation process, 2) The Secretary of State would need to review and certify specific election systems for use by county election offices, and 3) County officials would have to agree to purchase and implement the new Internet voting systems once they appear on the Secretary of State's list of Approved Election Systems.

Task Force Findings

Comprehensive vs. Incremental Approaches to Internet Voting

The Task Force recommends that any implementation of Internet Voting in the short-term be phased-in incrementally rather than comprehensively. The complete replacement of existing election processes would not be feasible for a number of reasons:

1) **Digital Identification.** A comprehensive Internet-based election system would require the use of a universally available form of digital identification that would allow election officials to verify both the identity and eligibility of potential voters. Although technology is capable of creating a universal digital identification system, that form of identification is not readily available and accessible to all voters.

2) **Voter Registration.** In the absence of digital identification, Internet-based voter registration is not secure. However, it may be possible to electronically revise and update voter registration information in the near future.

3) **Petition Signatures.** In the absence of digital identification and a digital voter roll, Internet-based digital signatures on initiative, referendum and recall petitions cannot be verified at this time.

4) **Voter Access.** Numerous state and federal laws and court precedents require that voting be accessible to all potential voters. Since not all voters have access to or a working knowledge of computers and the Internet, Internet voting should be used as an option to help improve voter turnout, not a barrier that would prevent participation.

This task force recommends that the adoption of Remote Internet Voting technology in the near term ought to be modeled on the California absentee ballot process. By requiring a voter to request an electronic ballot on paper, election officials will be able to compare the voter's signature on the electronic ballot application with the voter's signature on the voter registration card.

The use of the Internet Voting system in this scenario would be optional for voters , thus creating the potential for increased participation without creating any barriers to those who do not have access to or a comfort level with Internet technology.

Model of a Remote Internet Voting System

If the first contact an election official has with a potential voter is over the Internet, the election official would have no way to guarantee that the voter is

who he or she says he is. At the present time, the only reliable way to verify the identity of a voter in an Internet Voting application is to conduct a comparison of the voter's hand-written signature against the signature on the registration card previously filed at the elections office. Based on that comparison, the election official could then provide a digital signature to the voter whose signature matched the registration card.

A voter would then be able to use that digital signature to request and vote an Internet ballot.

A comparison between the paper absentee ballot process and a potential Remote Internet Voting system is demonstrated in the diagram below:

Paper Absentee Ballot Process

Voter registers to vote on paper voter registration card that is filed with county election office → Voter fills out and signs a paper "Absentee Ballot Request Form" → County Registrar of Voters verifies the signature on the "Absentee Ballot Request Form" → County mails absentee ballot to address specified by voter → Voter completes absentee ballot, signs outside of envelope and mails it to the county elections office → Registrar compares the signature on the outside envelope of absentee ballot to the voter's signature on the registration card → Registrar separates ballot card from the envelope and prepares ballot for counting → Absentee ballots are counted and merged with the votes from the precinct ballots.

Remote Internet Voting Process

Voter registers to vote on paper voter registration card that is filed with county election office → Voter fills out and signs a paper "Internet Ballot Request Form" → County Registrar of Voters verifies the signature on the "Internet Ballot Request Form" → County mails the digital signature to the voter at the address specified by voter → Voter uses key pair to access ballot over the Internet, completes Internet ballot and affixes the digital signature to the ballot before sending it over the Internet to the elections office → Registrar authenticates the digital signature and separates the ballot from the identifying signature information → Absentee ballots are counted and merged with the votes from the precinct and paper absentee ballots.

Implementation of Internet Voting

The Task Force recommends a phased-in approach to Internet Voting that would allow for a gradual testing of various components of technology required to authenticate voters and provide secure and secret ballots.

Each stage outlined below increases accessibility to Internet voting, but also creates additional challenges for election officials.

Phase One: Supervised use of an Internet Voting Machine

Stage One: Internet Voting at Voter's Polling Place

An Internet Voting Machine is used in a traditional polling place instead of a paper ballot. The polling place workers verify the identity of voters similar to current election procedures and provide the voter with an electronic ballot. The voted ballots are sent to election officials over the Internet and are tabulated by the county. Voters are required to vote at their home precinct.

Stage Two: Internet Voting at Any Polling Place

Same as Step One, except voters are allowed to vote at any polling place within a county or at centrally located Internet polling locations available to all voters in the county. The Internet Voting Machines are owned, maintained and protected by county elections officials.

County Controlled Infrastructure

Phase Two: Remote Internet Voting

Stage Three: Remote Internet Voting From County Computers or Kiosks

Voter is provided a password or digital signature from the county election officials and can use any polling place established throughout the community by the elections office. Poll workers are not necessary for voter authentication, so voting can take place at any time the Internet Voting Machines are open for use.

Step Four: Remote Internet Voting from Any Internet Connection

Same as Step Three, except in Step Four, voters would also be allowed to vote on their own computers as long as the operating system and web browser are protected from corruption. Election officials may provide voters with a single-use clean operating system and web browser for voting.

Infrastructure Not Controlled By County

Four Stages of Internet Voting

The task force finds that the development of a comprehensive Internet election system which would allow voters to conduct every step of the voting process over the Internet is not feasible at this time. The technical and procedural hurdles to producing such a broad ranging service at this time would be enormous.

This task force recommends that use of the Internet in elections should be phased-in gradually. The task force defines four different stages in the evolution toward Internet voting.

Each of the four stages of Internet voting are designed to provide greater convenience to voters, but each step also poses increasingly daunting technological and security concerns.

Some of the technical and security issues include:

- Voter Authentication
- Ballot Secrecy
- Ballot Integrity
- Reliable Vote Transport and Storage
- Prevention of Multiple Voting
- Defense Against Attacks on Internet Voting Machines
- Defense Against Attacks on Election Computer Systems

Stage One: Internet Voting Machines Used in Traditional Polling Places

The first stage of Internet Voting would allow voters to cast either an Internet ballot or a traditional paper ballot at their polling place. County election officials would be responsible providing secure Internet access in the polling place.

Essentially, at this step, Internet Voting will simply be a more complex form of the currently available electronic voting systems. It's primary value is in the early testing of technology that could eventually be used to allow voters to cast ballots from remote locations.

Who Is Served

Voters who cast their ballots at polling places.

Advantages

Provides voters with an easy to use election system.

Allows for the development and testing of the basic elements of an Internet Voting System that can eventually be used to allow Remote Internet Voting.

Voters are authenticated with traditional polling place protocols—technological authentication of voters is not necessary.

Stage One may be approved through the Secretary of State certification of an election system and may not require legislative authorization.

Implementation

Internet access would be required at polling locations. Counties may have a difficult time finding a sufficient number of acceptable polling places. Most traditional polling places, including residential garages, are not pre-wired to provide Internet access to four or five Internet Voting Machines.

Counties will incur substantial costs for the purchase of Internet Voting Machines/Computers.

Technical expertise will be needed to set-up, maintain, operate and eventually disassemble Internet voting machines.

Security Issues

All ballot transport and server-side security and failure tolerance issues must be resolved, including: encrypted ballot transport, failure tolerance for server infrastructure, defense against server attacks, certification of server software, procedures for vote canvass and procedures for audit and recount requirements.

All Internet Voting Machines must be protected against denial of service attacks which could threaten the voter's access to their ballot or their ability to transmit their ballot back to the elections office.

System Design Requirements

Prior to Voting

- Voter Registration Will Continue to Be Conducted on Paper for the Foreseeable Future

- Internet Voting Machines must be secured from attacks on the operating system. Potential computer attacks include malicious "Virus" or "Trojan Horse" computer code which could affect access to or the integrity of a voter's ballot. In this first stage of Internet Voting, the securing of the machines would be completed by election officials.

- Election officials must be able to prevent voters from casting more than one ballot in an election. Similar to the safeguards employed by election officials to prevent voters from casting both a precinct vote and a paper absentee ballot vote, procedures must be developed to ensure that voters are unable to cast multiple ballots using different voting methods.

Voting Process

- Voter will log on to the election system with a unique password that was assigned during the election official's authentication of the voter. In Stages One and Two of the implementation plan, voter authentication and voting machine preparation will be conducted by election officials at the polling place.

- After providing his/her password, the voter is presented with the appropriate ballot from county election server.

- Once the ballot is available on the voter's screen, the voter should be able to easily mark his or her preferences and review the voted ballot before it is transmitted to the county elections official.

- When the voter is satisfied that the ballot is marked correctly, the voted ballot is then submitted.

- The ballot is encrypted as it travels over the Internet to protect the secrecy and integrity of each vote.

- The ballot is received by the county election system which authenticates the validity of the vote, ensures that the vote has not been altered in transit

and automatically and immediately sends a receipt notice back to the voter.

****Processing of Ballots****

- Each vote is individually validated as a legitimate vote, separated permanently from the authentication information which previously tied the encrypted ballot to the voter and is stored for the vote canvass. Similar to a paper ballot placed in a ballot box, the Internet ballot is now impossible to tie to a specific voter.

- Voters may independently return to the county election site to confirm that his or her vote has been received and tallied, but because the ballots have been stripped of authenticating information by this point, voters will not be able to review the content of their own ballot after it has been voted.

- Votes are then counted and integrated into overall vote totals. As soon as the polls close on election day, the county elections officials will be able to tally all the Internet ballots and integrate the totals into the summary of votes cast by other voting methods (polling place and paper absentee votes).

- Votes are archived for recount and auditing purposes. Internet ballots, which have already been stripped of any code that could tie them to the voters who cast the ballots, should be archived for potential recount and auditing purposes.

Stage Two: Voter May Cast Ballot on Any County Controlled Internet Voting Machine. Election Officials Are Present for Voter Authentication.

Stage Two Internet Voting will allow voters to cast ballots over the Internet without visiting their own polling place. Voting would still occur on machines controlled by election officials and election officials would still conduct the authentication of voters, but voting can be made more accessible in this stage by allowing any voter in a county to vote on any Internet Voting machine. All ballot types will be available from all Internet Voting Machines.

Who Is Served

Polling place voters and voters who are unable to get to their home polling place during election day but may be able to visit a more convenient polling place during the day.

Advantages

All ballot styles will be available in all polling places, so voters would be able to vote at any Internet polling place in their county, not just their home precinct.

Implementation

Internet access would be required at polling locations. Counties may have a difficult time finding a sufficient number of acceptable polling places. Most traditional polling places, including residential garages and school assembly rooms, are not pre-wired to provide Internet access to four or five Internet Voting Machines.

New voting locations can be established at easily accessible locations such as malls, busy downtown office centers, universities, etc.

Counties will incur substantial costs for the purchase or lease of Internet Voting Machines/Computers.

Technical expertise will be needed to set-up, maintain, operate and eventually disassemble Internet voting machines.

Additional training will be required to ensure that poll workers are able to authenticate voters and provide the correct ballot style to voters from different precincts.

Security Issues

All ballot transport and server-side security and failure tolerance issues must be resolved, including: encrypted ballot transport, failure tolerance for server infrastructure, defense against server attacks, certification of server software, procedures for vote canvass and procedures for audit and recount requirements.

All Internet Voting Machines must be protected against denial of service attacks which could threaten the voter's access to their ballot or their ability to transmit their ballot back to the elections office.

The additional method of voting outside the voter's home polling place will make it more difficult to verify individual voters and check against double voting.

System Design Requirements

Prior to Voting

- Election officials must be able to authenticate all voters regardless of precinct. To provide voters with the option of voting from multiple locations within a county, poll workers should be given the appropriate tools to authenticate all voters within a county and ensure they are provided the correct ballot.

- Voter registration will continue to be conducted on paper for the foreseeable future.

- Internet Voting Machines must be secured from attacks on the operating system. Potential computer attacks include malicious "Virus" or "Trojan Horse" computer code which could affect access to or the integrity of a voter's ballot. In this second stage of Internet Voting, the securing of the machines would be completed by election officials.

- Election officials must be able to prevent voters from casting more than one ballot in an election. Similar to the safeguards employed by election officials to prevent voters from casting both a precinct vote and a paper absentee ballot vote, procedures must be developed to ensure that voters are unable to cast multiple ballots using different voting methods.

Voting Process

- Election officials will verify the eligibility of the voter to cast a ballot and identify the appropriate ballot style for the voter.

- Voter will log on to the election system with a unique password that was assigned during the election official's authentication of the voter. In Stages One and Two of the implementation plan, voter authentication and voting machine preparation will be conducted by election officials at the polling place.

- After providing his/her password, the voter is presented with the appropriate ballot from county election server.

- Once the ballot is available on the voter's screen, the voter should be able to easily mark his or her preferences and review the voted ballot before it is transmitted to the county elections official.

- When the voter is satisfied that the ballot is marked correctly, the voted ballot is then submitted.

- The ballot is encrypted as it travels over the Internet to protect the secrecy and integrity of each vote.

- The ballot is received by the county election system which authenticates the validity of the vote, ensures that the vote has not been altered in transit and automatically and immediately sends a receipt notice back to the voter.

****Processing of Ballots****

- Each vote is individually validated as a legitimate vote, separated permanently from the authentication information which previously tied the encrypted ballot to the voter and is stored for the vote canvass. Similar to a paper ballot placed in a ballot box, the Internet ballot is now impossible to tie to a specific voter.

- Voters may independently return to the county election site to confirm that his or her vote has been received and tallied, but because the ballots have been stripped of authenticating information by this point, voters will not be able to review the content of their own ballot after it has been voted.

- Votes are then counted and integrated into overall vote totals. As soon as the polls close on election day, the county elections officials will be able to tally all the Internet ballots and integrate the totals into the summary of votes cast by other voting methods (polling place and paper absentee votes).

- Votes are archived for recount and auditing purposes. Internet ballots, which have already been stripped of any code that could tie them to the voters who cast the ballots, should be archived for potential recount and auditing purposes.

Stage Three: Voter Authentication Code Provided by Elections Office Allows Voters to Cast Ballots at Any County-Controlled Internet Voting Machine

Stage Three of Internet Voting will allow voters to cast a ballot at any one of numerous unattended Internet Voting machines without the need for election officials to verify the identity of voters. For security purposes, the Internet Voting Machines must be secured from tampering and, although not staffed by election officials, should have technical assistance nearby. Voters would be able to vote around the clock well in advance of election day. In person-authentication of voters would be replaced by electronic authentication that requires advance planning by the voter.

Who Is Served

In addition to the voters who gained value from Stages One and Two, voters in Stage Three will be able to vote an Internet ballot up to 24 hours a day well in advance of election day without relying on election staff for authentication.

Advantages

With advance planning, the first step of voter authentication takes place through the elections office prior to election day by comparing the voters signature on an Internet ballot request form to the voter's registration card. Voters will now be allowed to authenticate themselves electronically without the assistance of county poll workers when they access an Internet Voting Machine in the community up to a month before election day.

Counties can borrow equipment and refer voters to numerous secure computers with Internet Access to improve the quantity and availability of voting locations.

Voters can vote near their home, workplace or school at any time.

Stage Three provides election officials with the opportunity to test the remote Internet voting authentication processes that will be used in subsequent stages of Internet voting.

Implementation

With no poll workers at the site, voters must receive prior approval via paper-based process and must obtain an authentication device from the elections office well in advance of voting over the Internet.

Voter education and training is critical for the success of Stage Three Internet Voting. Since voters may have technical difficulties, it will be important to have readily available technical assistance.

The process is more complex than most common Internet commerce transactions and may not be viewed as much more convenient for voters than current voting options.

Counties must develop a process for providing eligible voters with an electronic means of authenticating themselves to ensure that voters are able to access their ballot, but must also ensure that voters can only cast one ballot.

New Security Issues

Authentication system must be tied to a specific voter, but must be removed before the vote is tallied.

The authentication system must provide the public with assurances that only eligible voters will be able to obtain and vote a ballot.

Counties *must* verify the hand-written signature on each voter's Internet ballot request to the hand-written signature on the voter's registration card *before* providing the voter with an authentication code.

System Design Requirements

Prior to Voting

- Voter registration will continue to be conducted on paper.

- Internet Voting Machines must be secured from attacks on the operating system. Potential computer attacks include malicious "Virus" or "Trojan Horse" computer code which could affect access to or the integrity of a voter's ballot. In the Third Stage of Internet Voting, the securing of the machines would be completed by election officials or their technical representatives.

- To ensure that voters can obtain one and only one ballot when they access an Internet Voting Machine in Stage Three, voters will be required to request an Internet ballot authentication code from the county elections office. The request must be made on a paper Internet Ballot Request Form so the election official can compare the voter's hand-written signature on the request form to the hand-written signature on the voter's voter registration card.

  Since counties do not have any form of digital identification attached to the current voter registration cards, the election officials have no way to verify the authenticity of a voter's electronic request for an Internet ballot. For this reason, voters should not be allowed to request an Internet ballot electronically at this time.

The task force recommends that requests for Internet absentee ballots be made on paper and signatures should be verified against the paper voter registration card before Internet ballots and authenticating passwords or digital signatures are provided to voters.

- Once a county verifies the identity and eligibility of an Internet ballot requestor (voter) through a manual signature verification, the county approves the Internet ballot request and sends the voter information on how to authenticate himself on-line.

- The county election office must be prepared to provide all ballot types to voters. The county will be able to determine the appropriate ballot type for the voter based on the authentication code the voter uses to access the Internet Voting Machine.

- Election officials must be able to prevent voters from casting more than one ballot in an election. Similar to the safeguards employed by election officials to prevent voters from casting both a precinct vote and a paper absentee ballot vote, procedures must be developed to ensure that voters are unable to cast multiple ballots using different voting methods.

****Voting Process****

- Voter logs on to election system and authenticates him/herself. During Stages One and Two of the implementation plan, voter authentication and voting machine preparation is conducted by election officials at the polling place. In Stage Three, the voter independently requests an Internet ballot and is provided some form of authentication tool from the elections office. The voter can use that authentication tool to log on to the Internet election site to access the appropriate ballot.

- After providing his/her password, the voter is presented with the appropriate ballot from county election server.

- Once the ballot is available on the voter's screen, the voter should be able to easily mark his or her preferences and review the voted ballot before it is transmitted to the county elections official.

- When the voter is satisfied that the ballot is marked correctly, the voted ballot is then submitted.

- The ballot is encrypted as it travels over the Internet to protect the secrecy and integrity of each vote.

- The ballot is received by the county election system which authenticates the validity of the vote, ensures that the vote has not been altered in transit

and automatically and immediately sends a receipt notice back to the voter before the voter leaves the Internet voting machine.

Processing of Ballots

- Each vote is individually validated as a legitimate vote, separated permanently from the authentication information which previously tied the encrypted ballot to the voter and is stored for the vote canvass. Similar to a paper ballot placed in a ballot box, the Internet ballot is now impossible to tie to a specific voter.

- Voters may independently return to the county election site to confirm that their vote has been received and tallied, but because the ballots have been stripped of authenticating information by this point, voters will not be able to review the content of their own ballot after it has been voted.

- Votes are then counted and integrated into overall vote totals. As soon as the polls close on election day, the county elections officials will be able to tally all the Internet ballots and integrate the totals into the summary of votes cast by other voting methods (polling place and paper absentee votes).

- Votes are archived for recount and auditing purposes. Internet ballots, which have already been stripped of any code that could tie them to the voters who cast the ballots, should be archived for potential recount and auditing purposes.

Stage Four: Voter Authentication Code Provided By Elections Office Allows Voter to Cast a Ballot from Their Own Home or Office Computer

In Stage Four, voters will no longer rely on county-controlled equipment for Internet voting. Although, a paper Internet Ballot Request Form would still be required, voters would be able to use a county-provided authentication mechanism to vote from any computer with Internet access.

Who Is Served

Travelers, students, and others for whom it is easier to vote from any available Internet connection than it is to vote by mail or at a polling place.

Advantages

Voter convenience more closely mirrors the convenience experienced with other types of Internet transactions when voters can participate from virtually any Internet-accessible computer – not just from county-controlled Internet Voting Machines.

Voters can vote at any time of day from home, office or other location with Internet access.

The same computer voters use for studying ballot issues and candidates can also be used for voting.

Counties do not need to deploy Internet Voting Machines and support personnel throughout the community.

Disabled voters will have increased access to the voting process.

County-provided voting software would have limited functionality and would make voter's computer immune from viruses and other malicious software attacks.

Implementation

Substantial technical hurdles must be overcome and voters would be required to secure their own machines to guarantee security.

As in Stage Three, since no election official would be present during voting, the voter would have to manually request authorization for an Internet ballot through a paper request before voting.

It would be difficult to prevent political advertising from appearing on-screen and in the ballot window during voting if the voter's Internet Service Provider is one that displays advertising.

Voters must secure their platform: Voters would be inconvenienced by being required to "re-boot" the system in order to load a clean operating system to protect the computer against several types of electronic attack. Because of the clean operating system, voters may also have to reconfigure the computer to access their Internet Service Provider and return the computer to its original state after voting. This is considerably more complex than existing election procedures and is substantially more difficult that most Internet users experience in traditional Internet activities.

A large number of platforms need to be supported. There are many screens, video boards, key boards, mice, modems, network interfaces, and CD-ROM devices and, of course, both PC's and Apple Macintosh computers. The list will change quickly and will require the assistance of several major software and hardware companies and to remain current.

The market for voting software systems is relatively small. The development of complex Internet Voting software systems with numerous local variations capable of running on various machines and device configurations for a comparatively small-sized market may prove to be cost-prohibitive for either the vendor or the county.

Computers owned by third parties (neither the voter nor the elections officials) may be much more difficult to secure than home computers because they may reside behind industrial firewalls, they may be under the control of system administrators and they may not be suitable for their traditional business use when they are configured for voting purposes.

Institutional personal computers may be remotely monitored or controlled, possibly compromising ballot secrecy and/or integrity.

It will be essentially impossible offer phone support to help voters who have technical difficulties voting from institutional computers.

Vendors should prepare and counties will need to distribute an extensive instruction sheet for voters.

New Security Issues

Consumer PC's are extremely vulnerable to virus and other computer software attacks, either at the operating system or browser level. Such malicious software attacks can prevent voting, violate a voter's secret ballot, or even modify votes without the voter's knowledge despite the ability to encrypt ballots while they are transported over the Internet. Voters must therefore secure their own voting platform, but in the absence of county-provided, clean operating system and clean web-browser software, this requirement is difficult to enforce or detect.

There are a wide variety of computers, devices and Internet Service Providers (ISP's) in the marketplace that must be supported by any home or office Internet Voting software. It is extremely complex to develop software that not only works securely, but also can be operational on many different platforms.

The variety of home networking options is large and changing fast. Home local area networks, Internet connections that act like LANs, home firewalls and other unique systems create security complications that must be taken into account by software developers.

Voters working from the office, or other third-party controlled equipment, must assume, with no real way of checking that the computer is running standard software and is in a standard networking/Internet environment.

Depending on the institution involved, the computer may be controlled by remote control or monitoring software. If these types of software are present, ballot integrity and secrecy could be easily compromised.

Firewalls may prevent voting from some institutions and voters may be unaware of this limitation until they are prepared to cast their ballot.

System Design Requirements

Prior to Voting

- Voters must secure their Internet Voting Machine. One of the most significant threats to Internet voting is the potential of an attack on the operating system or other components of the computer used by the voter to cast an Internet ballot. An attack could take the form of a computer virus or other form of maliciously transmitted computer code designed to alter the performance of the computer.

  Such malicious code could create a variety of problems, including but not limited to: a computer crash which could prevent a voter from casting a ballot, alter a voter's ballot before it is encrypted or violate the secrecy of a voter's ballot without the voter's knowledge.

  To protect against an attack, voters would be asked to take some form of security steps to minimize risk. The complexity of such steps may be simple or complex, but may include the installation of a clean, uncorrupted operating system and/or a clean Internet browser to ensure that the voter is not subject to browser-based advertising or electioneering during the voting process.

Although this step would not be necessary for voters using a secure Internet voting kiosk maintained by the county elections office, it is very important for voters using home computers.

- Voters need to understand the limitations of Internet Voting Machines that reside behind a company firewall. Voters may find that the computer they intended to use to access their Internet ballot process is unable to receive and transmit the encrypted ballots through a network firewall. Voters should be sure they are able to vote from their preferred computer before relying on the Internet to cast a ballot.

- Voter must assume a standard software/networking and Internet environment on office or public computers. Because software is placed on these systems by persons other than the voter or election officials, the voter must trust the system does not include software capable of preventing, reading or altering the voter's ballot.

- Voters should be aware of the potential breach of ballot secrecy on networked computers. Voters should recognize that some network administrators have the ability to remotely monitor computer transactions. Although ballots are encrypted and protected once they are sent over the Internet, it is possible for monitoring or "remote-control" software to read or alter an unencrypted ballot while it is housed on the voter's computer. Severe civil and criminal penalties should be adopted to deter computer network administrators from violating the secrecy or integrity of a voter's Internet ballot.

****Voting Process****

- Voter logs on to election system from any Internet accessible computer and authenticates him/herself. During Stages One and Two of the implementation plan, voter authentication and voting machine preparation is conducted by election officials at the polling place. In Stage Four, as in Stage Three, the voter independently requests an Internet ballot and is provided some form of authentication tool from the elections office. The voter can use that authentication tool to log on to the Internet election site to access the appropriate ballot.

- After providing his/her password, the voter is presented with the appropriate ballot from the county election server.

- Once the ballot is available on the voter's screen, the voter should be able to easily mark his or her preferences and review the voted ballot before it is transmitted to the county elections official.

- When the voter is satisfied that the ballot is marked correctly, the voted ballot is then submitted.

- The ballot is encrypted as it travels over the Internet to protect the secrecy and integrity of each vote.

- The ballot is received by the county election system which authenticates the validity of the vote, ensures that the vote has not been altered in transit and automatically and immediately sends a receipt notice back to the voter before the voter logs off of the Internet voting machine.

****Processing of Ballots****

- Each vote is individually validated as a legitimate vote, separated permanently from the authentication information which previously tied the encrypted ballot to the voter and is stored for the vote canvass. Similar to a paper ballot placed in a ballot box, the Internet ballot is now impossible to tie to a specific voter.

- Voters may independently return to the county election site to confirm that their vote has been received and tallied, but because the ballots have been stripped of authenticating information by this point, voters will not be able to review the content of their own ballot after it has been voted.

- Votes are then counted and integrated into overall vote totals. As soon as the polls close on election day, the county elections officials will be able to tally all the Internet ballots and integrate the totals into the summary of votes cast by other voting methods (polling place and paper absentee votes).

- Votes are archived for recount and auditing purposes. Internet ballots, which have already been stripped of any code that could tie them to the voters who cast the ballots, should be archived for potential recount and auditing purposes.

Task Force Findings and Recommendations on Policy Issues

Additional Convenience to Voters May Help Improve Participation

While it has been conventional wisdom that anything that makes voting easier, even easier voter registration through the "motor voter" legislation, will increase voter turnout, the reality is that making it easier to register has not increased voter turnout at the national level or in the state of California. Although the restrictive voter registration procedures which were implemented in the late 19th century did have the effect of reducing overall voter turnout in presidential elections from 79 percent of the eligible voting age population in 1896 to 49 percent of the eligible voting age population in 1920, turnout began to increase again despite these restrictive registration requirements until it reached a 20th century peak of 65 percent in 1960. However, from 1964 forward, despite less restrictive registration requirements in many states and increasing education levels across the country, voter turnout once again began to erode. Even the National Voter Registration Act of 1993 (the "motor voter bill") that simplified registration and prevented removal of names from registration rolls for failure to vote, did not increase turnout. In fact from its implementation date in 1995, voter turnout has generally declined. In California, 54.52% of the voting age population voted in the presidential election of 1992, however, in the next presidential election in 1996 only 52.56% of the voting age population turned out. The same trend was manifested in the off-year elections of 1994 and 1998; turnout decreased from 46.98% of the voting age population in 1994 to 41.43% of the voting age population in 1998.

However, Internet voting, if implemented would do more than simply ease the method of qualifying to vote, it would make the act of voting easier for anyone who has access to the Internet. Here then we may see an increase in voter turnout based upon the combined approaches of easier voter registration ("motor voter") and more efficient voting procedures.

Since two major groups of low-propensity voters --- those who are young 18-25 year old students or busy professionals who do not find the time to participate are also two of the more Internet savvy segments of the population, we anticipate that the introduction of Internet Voting, specifically remote Internet Voting, would provide a positive effect on turnout.

<u>Use of the Internet is Continuing to Increase and Home Use May Eventually Rival Use of the Telephone and Television</u>

Many pundits are predicting that the Internet will have an impact on the political process that will rival the effect television has had on our elections. If the impact of the Internet on elections is roughly similar to the impact the Internet has had on commerce, then the results would indeed be staggering.

The University f Texas estimated that approximately $102 billion in US revenue was transacted over the Internet in 1998. This number is projected to reach $1.1 trillion in the year 2002.

As the public looks to the Internet to provide convenience in commerce and in preparing for elections, it appears likely that given the opportunity to vote on a *secure, trusted* system, many people who are eligible to vote would cast their ballots on-line. It is also reasonable to assume that many people who use the Internet today, but have not historically participated in the election process may be attracted to participating in an on-line election.

Similar to the way in which the ceremonial gathering of neighbors in a suburban garage prompts people to wander down the street to vote, an on-line election would create a major Internet event that may prompt regular Internet users to participate, if for no other reason than it is the major happening in the cyber-world for that day, week or month.

Voter Accessibility to the Internet

Current and Projected Access

One of the primary factors that could limit the widespread acceptance of Internet voting in the immediate future is the availability of Internet access to the voting public. To ensure equity for all eligible voters, election officials should ensure that computer ownership and Internet access are not insurmountable barriers to Internet voting.

Deployment of Internet technology worldwide has taken place much more rapidly than the deployment of technologies that are considered to be ubiquitous today. For example Morgan Stanley Technology Research reports that it took 38 years from introduction for the radio to gain acceptance and be adopted by 50 million users. It took 30 years for the telephone, 16 years for the personal computer and 13 years for the television, each to be adopted by 50 million users. The Internet reached 50 million users in only 4 years.

In the US, the home has been the main point of Internet access since 1994, followed by the workplace. By the end of 1997, 42% of US households had a home-PC and about 22% had Internet access at home. [Source: Dataquest and The Yankee Group]. The user base is shifting away from the technologically advanced early adopters and becoming more representative of the population as a whole. Two main factors are responsible for this shift [Source: IDC and Dataquest]:

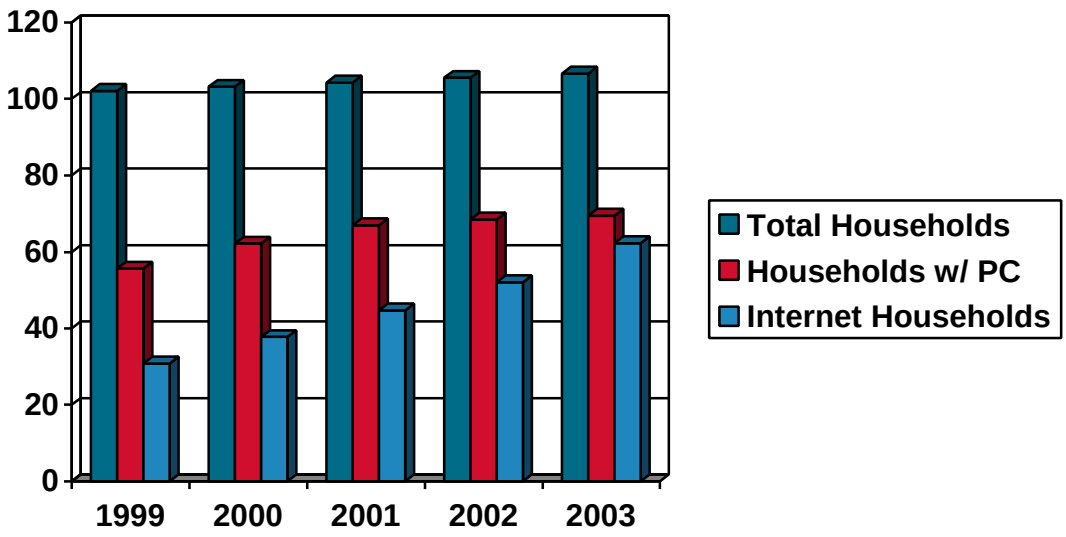
- The shift to flat rate pricing at the end of 1996. This effectively took the Internet "off the meter" and encouraged use by those with lower or fixed incomes and those not working.

- The rapid expansion of Intranets in the workplace, particularly since 1996. This led to a higher proportion of young women using the Internet for the first time.

However, a recent study by the U.S. Department of Commerce suggests that income is still a significant factor in the availability of Internet access in American households. As the price of computers and Internet Service Providers decreases, that gap is expected to shrink.

A December 1999 survey conducted by the Public Policy Institute of California reported that only 20.3 percent of California households with an income under $20,000 had frequent (often) access to the Internet. In the $20,000-$39,999 income bracket, 31.2 percent of households accessed the Internet and/or email often. By contrast, more than 72 percent of households with an income in excess of $80,000 enjoyed similar Internet access.

Projected American Households with Internet Access (Millions)
(Source: Dataquest and The Yankee Group)



As the chart above depicts, there are steady growth projections for the number of households with computer devices (24.8% growth; 1999 – 2003); and significant growth projected for the number of households with Internet access (102.3% growth; 1999 – 2003). This growth reflects an increase in the percentage of US households with Internet access from 30.2% in 1999 to 58.4% in 2003.

In addition, there has been a steady increase in the proportion of users accessing from the workplace only, driven by the rapid expansion of Intranets.

There has been an even more rapid increase in the proportion using the Internet only from “other" (indirect) locations - such as schools, libraries and friends' homes. By mid-1998, 58% of all adult Internet users had access from home - a proportion that has fallen from 75% in 1994. By 2005, it is forecast, just over 95% of PC-owning households in the U.S. will have direct or indirect Internet access.

Public Access to Internet Connectivity Should Be Made Available in Counties that Adopt Internet Voting Systems

Until such time as Internet connectivity becomes nationally ubiquitous some form of reasonable access should exist for those voters without connectivity in their homes or places of work. Programs that could increase Internet voting access could include the following:

1) Kiosk or transportable computer that is designed, dedicated and available exclusively for voting;

2) Computer already installed in a public facility that can be made available to the voting public during an election period.

A kiosk or transportable computer dedicated to voting represents a traditional approach to providing a polling place with the tools required for voters to gather and participate in an election process. However there are many logistical and financial barriers to making this a workable and practical solution. In addition to the cost and up-keep of the computers required to provide Internet Voting access in a polling place, there is the requirement of providing an Internet connection from the polling place. At a minimum, Internet connectivity would require prior arrangements and/or access to a dedicated telephone or other acceptable access line, plus the cost of the access and the installation of the line and the computer.

Alternatively, computers installed in publicly accessible facilities may be an acceptable solution to provide access for members of the voting public who do not otherwise have access to an Internet connection. Such publicly accessible facilities may include but not necessarily be limited to the following: elementary or secondary schools; public libraries; public housing centers; Employment Development Department job centers; National Guard centers; university, college and community college libraries. All such facilities are or soon will be equipped with computers and Internet connectivity, but not all may be appropriate as Internet polling places.

Facilities where computers are installed for administrative, operational or educational purposes may not be accessible to the public or appropriate as polling places. However, computers installed for the purpose of providing access to reference or research material may be appropriate for use as Internet Voting machines that can be made available to the public.

If computers in public facilities are to be used as Internet Voting machines consideration must be given to ensuring the privacy of the voter. Precinct polling locations in a traditional non-Internet election provide polling booths with curtains or other physical barriers to protect voter privacy. Similar devices should be employed when Internet Voting machines are located in open areas and are visually accessible from the front and/or sides to protect the voter's privacy from the infringement of others.

Eventually, when remote Internet Voting is available, physical voting privacy should also be protected at any location where voters may be casting their ballots, including workplace computers or computers that may be regularly monitored by security cameras.

Characteristics of an Internet Voter

The task force is unable to specifically quantify the effect that the various stages of Internet Voting might have on voter turnout, but we are encouraged that many of the individuals who are least likely to participate in the current elections process are also the most likely to use the Internet.

The Federal Elections Commission reports that the age group that is least likely to vote is the group aged 18-24. During the 1996 elections, less than one-third of 18-24 year olds cast a ballot for president. By contrast, in that same election more than 54 percent of the overall population went to the polls.

In part due to the availability of the Internet in schools, Internet access among that same 18-24 age group is considerably higher than the rest of the population. The Public Policy Institute of California reports that 73 percent of 18-24 year old Californians either often or sometimes have access to the Internet and email.

Another likely beneficiary of the increased convenience afforded by Internet Voting is the occasional voter who neglects to participate due to a busy schedule and tight time constraints. If voting is made more accessible for these voters during the course of their already hectic days, they might be more likely to participate.

Unfortunately, the benefits gained by providing Internet Voting access to these voting groups may be negated by the cumbersome process and advanced planning that would be required to ensure a secure and secret remote Internet ballot as described in this report.

These benefits are most likely to be realized if and when a simplified form of digital identification is universally available that would allow the entire voting process to take place over the Internet, from registration – to Internet ballot request – to voting.

Public Acceptance of Internet Voting

It appears that younger voters would be more likely to participate in our elections than they do today if they are given the opportunity to vote over the Internet. The December 1999 survey from the California Public Policy Institute shows that younger voters are more likely to have Internet access and more likely to support Internet Voting than older voters. (Appendix B)

That assumption is further confirmed by a July, 1999 ABC News poll which showed that 61 percent of potential voters aged 18 to 34 would be willing to vote over the Internet if it could be made secure, whereas 42 percent of the overall population expressed a similar comfort level with secure internet voting.

Although the ABC News poll finds that 24% of Americans believe that Internet voting "could be made secure from fraud anytime in the near future," fully 69% of all Americans think that making Internet voting secure from fraud will take "many years" or will "never happen." Further, 60% of all 18-34 year olds agree, stating that it will be "many years" before Internet voting will be secure.

However, we may see slightly more support for Internet voting in California, as the ABC News polling data show that 50% of those in the West support Internet voting if it could be made secure, and 27% in the West believe that it could be made secure from fraud "in the near future."

Internet vs. Paper Ballot Voters

The recent ABC news nationwide poll indicates that currently only 19% of the population of Americans who are over 65 would support Internet voting even if it could be made secure from fraud. These numbers indicate that any Internet voting system would have to make an effort to increase the comfort level of the elderly population.

The gradual implementation of Internet Voting recommended by the task force will help ease the transition for those who may be concerned about the new technology. The retention of the paper ballot process should also guarantee voters who are uncomfortable with the new technology that they will still have access to their preferred alternative method of voting.

The Polling Place Internet Voting system described in Stages One and Two of this report may serve as more than just a trial run to determine cost, and potential problems, but could also help to acclimate the older population and reassure Californians in general that vote security and voter secrecy are not insurmountable problems, but rather have been dealt with in a trustworthy and

professional manner. The ability to conduct audits of the Internet vote would be crucial to building this public trust.

Need for voter education regarding the integrity, security, and privacy of Internet voting.

Accordingly, the public must be kept apprised of the manner by which the Internet is protected from outside influences, including national and international hackers as well as individual voters who might try to cast more than one ballot. Additionally, it is imperative that all voters are assured that their right to a secret ballot is protected and guarded jealously by government officials who themselves are kept aware of *who* has voted, but purposely are kept ignorant *how* individuals vote. This then is the fine line that those who administer Internet voting must walk – audits must be possible, fraud must be impossible, and the secrecy of ballots must be ensured.

The administration of the Internet voting process by election officials should be observable by the public and interested parties.

To continue to ensure voter trust and the legitimacy of governments elected with Internet votes, all levels of the Internet voting process must be observable and observed by the public and interested parties. Additionally, official monitoring should be implemented to speak to the authenticity of the resulting vote.

Important Design Elements

All voting systems must include several design elements to satisfy legal requirements and ensure the integrity of the election.

An Internet Voting system must ensure the following:

- *Ballot secrecy*
  Absolute secrecy of the ballot is a fundamental requirement of all election systems. Secrecy should be provided during the voting process, while the vote is en route to the election official over the Internet and after the ballot has been received. At least the same level of secrecy provided in paper absentee ballots must be met.

- *Ballot security*
  Each individual vote must be protected and should be unalterable once the voter sends the ballot to the elections official. The election office's computers should secure and protected against physical or technological attack.

- *Vote tabulation accuracy*
  The accuracy of the vote count should be unassailable.

- *Internet voting systems shall be user friendly and offer voters a simple, convenient and uncomplicated opportunity to vote*

- *Internet ballots should be free of any political or commercial advertising on either the web page or the web browser*

- *Internet voting systems should comply with the Federal Voting Rights Act*
  The Federal Voting Rights Act of 1965, As Amended, was enacted for the purpose of ensuring that no voting qualifications or procedures are imposed that would have the effect of abridging or denying voting rights to citizens based on account of race or color. In four California counties, this Act requires pre-clearance from the U.S. Department of Justice for any voting changes before the changes are implemented in any of those four counties. Any Internet voting system which is proposed in California, must ensure that the ballots of minority voters are not adversely affected.

- *Internet voting systems should allow election officials to conduct a 1% manual recount of ballots and provide election officials with an audit trail for recounts and election contests*
  For voter trust to remain intact, votes must arrive at the election office's canvassing computers unscathed. Accordingly, the system must be incapable of breach or error in authentication, secrecy and integrity. It must have audit capability built in to the system design.

- *Internet voting should be accessible to voters with disabilities*
  The design of an Internet Voting system should take steps to maximize the accessibility of voting to persons with disabilities.

- *Voters should receive appropriate disclosures prior to casting their ballot*
  If the configuration of a voter's computer network prevents election officials from guaranteeing the secrecy of a ballot, the voter should be informed that his or her vote may be witnessed by his network administrator even though such an invasion of a voter's ballot secrecy would constitute a crime. The voter would then have the option of proceeding with his or her vote or contacting election officials to obtain a paper ballot.

- *Internet ballots should be available in the same languages required by the Federal Voting Rights Act and any applicable state or local law*

Procedural Differences Between Precinct, Paper Absentee Internet Voting

The Task Force has identified several differences between paper and electronic Internet ballots that warrant policy review prior to adopting an Internet Voting System.

Electronic ballots provide opportunities to improve the efficiency of the voting process and include safeguards that could prevent voters from making common mistakes that force election officials to disregard their ballots. While many members of the Task Force believe that we should not intentionally incorporate the weaknesses of the paper ballot into the design of an electronic system, others are concerned that giving Internet voters a superior voting system would be unfair to voters who make mistakes on the paper ballots. It should be noted that solutions to some of the imperfections in the paper system have already been incorporated into electronic voting systems that have been approved by the California Secretary of State.

- *Over-voting*
  An Internet ballot can be designed to prevent voters from casting a vote for more candidates than they are allowed in a given race. In the paper system, a voter who votes too many times in one race has his entire vote for that race disregarded.

- *Skipped contests*
  Voters often intentionally or unintentionally skip contests they are eligible to vote in on paper ballots. The Internet ballot can be designed to warn voters when they skip a contest, but it should never require a voter to vote in each race.

- *Write-in candidates*
  An Internet voting system must include a process by which the Internet voter may write-in the name of a candidate for an office and vote for that candidate if he or she chooses to do so.

- *Links to official candidate statements and ballot pamphlets*
  While the Task Force recognizes the benefits of using the Internet to help educate voters, we are leery of including links to web sites that voters could access during the voting process which are not directly maintained by the elections officials. The current ban on electioneering during the voting process should be maintained as closely as possible during Internet voting.

- *Availability of technical voter assistance*
  In the polling place voters may ask precinct officials for assistance in the mechanical voting process. Voters who cast absentee ballots are able to call the elections office with questions. But, Remote Internet Voters may have technical questions that need to be directed to technical experts rather than election officials. Voters who access the Internet from home also may be unable to call a help line while they are connected to the Internet if they only have one phone line in their household. Technical assistance should be available both on-line and on the pone. Answers to frequently asked questions and sample technical problems should available on-line and in the printed ballot pamphlet.

- *Public roster of voters who have and have not cast ballots*
  A list of voters who have voted in a given election is generally available to political campaigns to assist in their efforts to get out the vote. This information could be much more widely accessed over the Internet. A decision should be made regarding the ease with which this information should be made available electronically to the general public.

Revising Election Laws to Accommodate Internet Voting

- *Electioneering*
  Current laws that prevent electioneering at the polling place and during absentee voting should be expanded to prohibit electioneering during Internet voting, especially since a large number of Internet voters may access their ballots on a computer terminal in a public place, such as a library or public Internet kiosk.

- *Voting in the workplace*
  For many voters, their primary method of access to the Internet will be from the workplace. Legislation should be considered to ensure stiff penalties against any employer who intentionally monitors the ballots of his or her employees via electronic means or visual surveillance while the employees are voting on the Internet, as well as employers who engage in electioneering, coercion or vote tampering in an effort to influence their employees' votes.

- *Strong penalties should be specified for fraud, abuse, tampering and violation of a voter's right to a secret ballot*
  Current law specifies the penalties for a variety of election-related violations. These laws, especially as they pertain to voter fraud, vote tampering, and interfering with the voter's right to a secret ballot, should be extended to Internet voting as well.

- *The State Legislature should appropriate funds to pay for the initial cost of initiating Internet voting systems for each county that chooses to adopt Internet voting.*

Appendix A

Technical Committee Report

Appendix B

Public Policy Institute of California Statewide Survey: Californians and Their Government, December 1999

Do You Favor or Oppose Internet Voting?

Age	Favor	Oppose	Don't Know
18-24	60	37	3
25-34	59	37	4
35-44	52	43	5
45-54	48	47	5
55-64	37	58	5
65+	20	71	9

########

Do You Have Access to the Internet and/or email?

Age	Yes/Often	Yes/Sometimes	Never
18-24	50	23	27
25-34	53	17	30
35-44	48	22	30
45-54	49	18	33
55-64	37	20	43
65+	16	10	74