VOTING SYSTEMS TASK FORCE

Edwin M. Lee, Mayor

DRAFT FOR PUBLIC COMMENT

Recommendations on Voting Systems for the City and County of San Francisco

A Report by the San Francisco Voting Systems Task Force (VSTF)

Public Comments Are Invited

This report provides strategic guidance to assist the City and County of San Francisco as it considers its next voting system. The report is not intended to be a complete statement of requirements or technical specifications, and is not an exhaustive study of all topics related to voting systems. The VSTF eagerly invites comments from the public, and will consider all comments received within the VSTF scope of work.

Submit Comments by Email:
voting.systems.task.force@sfgov.org

Submit Comments by Mail:
Voting Systems Task Force
City Hall, Room 362
1 Dr. Carlton B. Goodlett Place
San Francisco, CA 94102

Comments due by 5 pm on March 2, 2011

Table of Contents

Section 1: Introduction and Background – p. 3

Mission and Context of the Voting Systems Task Force (VSTF)

Background on San Francisco's Current Voting System

Opportunities Presented by Next Generation Voting Systems

Section 2: Recommendations – p. 6

Election Records and Post-Election Audit Procedures – p. 7

Balloting Systems and Services – p. 15

Security – p. 23

Acquisition Strategies – p. 32

Section 3: Appendix – p. 38

A: Concerning the Ranked-Choice Voting Manual Tally Process Currently Used in the City and County of San Francisco

B: Ranked-Choice Voting Considerations

Section 4: About the VSTF – p. 40

Section 1
Introduction and Background

Mission and Context of the Voting Systems Task Force (VSTF)

In September 2008 the San Francisco Board of Supervisors established the Voting Systems Task Force to make recommendations to that body about voting systems standards, design, and development (Ordinance 268-08; www.sfbos.org/ftp/uploadedfiles/bdsupvrs/ordinances08/o0268-08.pdf).

The VSTF defines its work as follows:

Mission: The VSTF's mission is to advise the City and County of San Francisco on the development and/or acquisition of voting systems that ensure fair and accurate elections, achieve voter intent, and provide for transparency and public auditability of voting systems components and election data.

Scope and Objective: Activities encompass voting systems and related elections issues that affect or are affected by voting systems and voting system acquisition in the City and County of San Francisco. A "voting system" for this report is defined to be a system of hardware, software and processes which prepares a ballot and records, collects, transmits, counts, and reports on votes and election results as cast by voters. Included in this definition are the associated reports and audit logs which provide information about management of election data in the system and system use, integrity, administrative access, configuration and configuration changes as well as documentation for support, use and training on use of the system.

The VSTF report contains recommendations, with supporting rationale, for each of the five areas identified by Section 5.405(b) of the Administrative Code. Recommendations have been collapsed into four topic areas: election records and post-election audit procedures; balloting systems and services; security; and acquisition strategies. This report provides strategic guidance and minimum requirements to assist the City and County of San Francisco as it considers its next voting system. The report is not intended to be a complete statement of requirements or technical specifications, and is not an exhaustive study of all topics related to voting systems. The Board of Supervisors may wish to initiate further investigation of certain topic areas as it considers a direction for San Francisco's next voting system.

Timeframe for Recommendations: San Francisco is currently under contract with Sequoia Voting Systems, and has the option to extend that contract through elections in 2013. The VSTF has identified several opportunities for improving public confidence in the City's use of Sequoia Voting Systems. However, this report primarily suggests minimum requirements for the City and County of San Francisco's next voting system (to be implemented for elections in 2014, if feasible). VSTF recommendations can be found in Section 2 of this report.

Audiences: Our recommendations are intended to provide guidance to a variety of audiences including:

- the San Francisco Board of Supervisors
- the Department of Elections
- the Elections Commission
- San Francisco voters

Background on San Francisco's Current Voting System

On March 31, 2005, the City and County of San Francisco Department of Elections (DOE) initiated a Request for Proposals (RFP) process seeking bids for a new voting system, including equipment and services, to collect, count, tabulate, and report votes (see DOE RFP for a New Voting System at http://www.sfgov2.org/index.aspx?page=1869). In December 2007, the San Francisco Board of Supervisors approved a contract with Sequoia Voting Systems for voting systems/services (http://www.sfgov2.org/Modules/ShowDocument.aspx?documentid=152). Sequoia replaced Elections Systems and Software (ES&S) with which the City had been under contract through the 2007 election cycles.

The Sequoia system was implemented beginning with the February 2008 election. The contract runs through December 2011. The contract with Sequoia Voting Systems for a voting system and associated services is valued at $12,650,233.35 (see Resolution 654-07). The DOE has the option to renew the contract two times, each time for one year and has indicated that it anticipates extending the Sequoia contract through the end of 2013. Were it to do so, the DOE estimates that annual maintenance would be approximately $400,000, and services per election would be approximately $500,000. With three elections scheduled in 2012, the projected cost would be approximately $1.9 million. With one election scheduled in 2013, the projected cost would be approximately $900,000 (two year total: $2.8 million)

Opportunities Presented by Next Generation Voting Systems

The City and County of San Francisco is prudent to begin considering the characteristics of the voting system it would like to implement after its contract with Sequoia terminates, and to consider whether a new acquisition model is feasible. In fact, the City is in good company. Across the nation, jurisdictions are grappling with how to provide elections that are accurate, fair, secure, transparent, and accessible, and with how to evaluate the merits of various systems and acquisition models. The conversation about next generation voting systems is becoming increasingly robust and is generating opportunities for collaboration and information sharing. An effort to study future voting systems has been undertaken by at least two other jurisdictions including:

County of Los Angeles (California) Voting Systems Assessment Project (VSAP)
http://www.lavote.net/voter/VSAP

Travis County (Texas) Elections Study Group 2009
http://www.co.travis.tx.us/county_clerk/election/study_group_2009

The San Francisco Department of Elections (DOE) under the capable leadership of Director John Arntz has run smooth elections by establishing best practices and security protocols. Yet, the VSTF believes that there is room to improve the underlying voting system and the procedures that accompany the elections process. The VSTF has identified opportunities for improvement in several core areas:

- intent of voter and accessibility
- audit and verification procedures
- security
- transparency

At the heart of the challenge is the current nature of the private vendor marketplace, which is characterized by a lack of competition, restrictive vendor contracts, and undisclosed software code. This situation is compounded by a challenging and costly regulatory structure which further constrains innovation. The VSTF believes that the City and County of San Francisco should be an active participant in the movement toward more transparent voting systems, and should consider a broad range of possibilities regarding the business and partnership model it will pursue to acquire/develop San Francisco’s next voting system. This could include collaborating with other jurisdictions, academic institutions, or non-profit organizations.

The VSTF has framed its recommendations to address the core challenges described above. While a flawless voting system ~~in not~~ attainable, VSTF members hope that this strategic guidance will help the City and County of San Francisco move toward a system that earns the highest level of public confidence.

SECTION 2

RECOMMENDATIONS

This report is intended to provide strategic guidance and minimum requirements to guide the City and County of San Francisco's as it considers its next voting system. Recommendations encompass four primary topic areas: election records and post-election audit procedures; balloting systems and services; security; and acquisition strategies.

Within some topic areas, the VSTF has identified actions that can be implemented in the short-term for improving public confidence in the City's current use of the Sequoia Voting System.

ELECTION RECORDS AND POST-ELECTION AUDIT PROCEDURES

Introduction

This section concerns the records generated in the course of an election and the procedures for checking records to verify that the election was conducted properly. Comprehensive records and audit procedures are essential for ensuring a correct outcome, deterring fraud, building public confidence in elections, and understanding how to improve the election system. Though there are many types of audits, this section deals only with post-election verification of the results.

Definitions and Concepts

Election records include paper or electronic records at all stages of an election, such as:

- **Voter registrations**: lists of the registered voters
- **Election definitions**: lists of the contests and candidates in the election and which groups of voters are eligible to vote in which contest
- **Ballot definitions**: descriptions of the contents and layout of each type of blank ballot
- **Cast vote records** (CVRs): electronic records of the choices that a voter made
- **Audit logs, event logs, and error reports**: timed records of events that took place during the election (e.g., accessing of sensitive information, opening or closing of polls, casting of ballots, granting or revocation of access, actions by election workers)
- **Canvass records**: all records used to reconcile vote totals during the post-election canvass period (period between election night and the date an election is certified), including ballot reconciliation sheets, records establishing chain of custody, and other precinct records.
- **Vote counts**: counts of the votes (usually within an election district)
- **Election outcome**: the winning candidate in a contest, or the winning side of a referendum, as determined by the vote counts from all districts
- **Election results**: the final report of overall vote counts and outcomes, including number of ballots cast, voter registration and voter turnout percentages and other detailed election statistics

A **post-election audit** is a procedure conducted after an election to check the vote counts. It is usually performed by dividing the cast ballots into groups called **audit units**, selecting some fraction of the audit units for a manual count, and checking that the manual counts for each unit match the vote tallies from the election.

Any post-election audit procedure that ensures a high, pre-specified chance of detecting and correcting an incorrect election outcome is called a **risk-limiting audit**. Audits can be made risk-limiting by establishing specific criteria under which a full recount must occur. For example, to limit the risk of an incorrect outcome to 1%, the audit procedure must have at least a 99% chance of escalating to a full recount when the outcome is incorrect.

Ranked-choice voting (RCV) is an election method in which each voter indicates a first choice, an optional second choice, and an optional third choice for an elected office. In the first round of counting, all ballots are assigned to their first choices. If one candidate now has a majority of the ballots, that candidate wins. If not, the candidate with the least ballots is eliminated; ballots with that candidate as their first choice are then reallocated to their second choice, or set aside as exhausted ballots if there is no second choice. Rounds of counting and elimination repeat, always assigning each ballot to its highest-ranked non-eliminated candidate, until one candidate has a majority of the non-exhausted ballots.

Election Markup Language (EML) is a suite of XML-based data formats for election records, defined by the Organization for Advancement of Structured Information Standards (OASIS). The current version is EML 5.0 and work on EML 6.0 is under way. EML defines several different data formats for different kinds of records; each format is identified by a number.

Findings

Voting system reliability

Numerous independent investigations have discovered serious security weaknesses and design errors in widely used electronic voting equipment. To cite some examples:

- In 2004, four computer security experts examined the source code of a DRE voting machine [1] and found it to be “far below even the most minimal security standards applicable in other contexts.”
- In 2006, investigators at Princeton University demonstrated that it is possible to construct a software virus that spreads from voting machine to voting machine, while altering votes in an undetectable fashion[2].

[1] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach (2004). Analysis of an Electronic Voting System. In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press.

- In 2007, a team of reviewers appointed by the California Secretary of State found major security flaws in all three of the major brands of voting systems used in California[3][4][5], including vulnerability to infection by a software virus in some cases.
- In 2008, the election system in Humboldt County erroneously deleted 197 ballots[6].

Voting machines continue to be perceived as untrustworthy in the public consciousness. The investigations mentioned above were widely publicized, and there continues a steady flow of news headlines raising concerns about flaws and reliability problems with voting machines.

Finding 1. It is not safe to rely solely on electronic voting equipment for accurate results.

Finding 2. Public confidence in electronic voting has weakened in recent years.

Current auditing procedures

San Francisco's post-election audit is known as the "1% Manual Tally," in which the ballots from a random selection of precincts are manually recounted.[7] The manual counts are checked against machine reports at the precinct level. For speed and accuracy, the contests are counted one at a time; that is, each counting team counts a single contest for an entire precinct, then counts the next contest for the entire precinct, and so on.

We inquired as to the procedure taken when the audit appears to be at variance with the reported election results. When there is a discrepancy of even one vote, the ballots are counted again, with particular attention to counting the ballots as a machine would count them, not as a human would interpret the voter's intent. That is, the audit seeks a way to interpret the ballots that confirms the machine result. If a discrepancy remains after a second count, the audit team fills out a Manual Tally Incident Report, which reviewed by supervisors in charge of the canvass.

[2] Ariel J. Feldman, J. Alex Halderman, Edward W. Felten. *Security Analysis of the Diebold AccuVote-TS Voting Machine*. URL: http://citp.princeton.edu/pub/ts06full.pdf

[3] Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David A. Wagner, Harlan Yu, and William P. Zeller (2007). *Source Code Review of the Diebold Voting System*. URL: http://www.sos.ca.gov/voting-systems/oversight/ttbr/diebold-source-public-jul29.pdf

[4] Srinivas Inguva, Eric Rescorla, Hovav Shacham, and Dan S. Wallach (2007). *Source Code Review of the Hart InterCivic Voting System*. URL: http://www.sos.ca.gov/voting-systems/oversight/ttbr/Hart-source-public.pdf

[5] Matt Blaze, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, and Ka-Ping Yee (2007). *Source Code Review of the Sequoia Voting System*. URL: http://www.sos.ca.gov/voting-systems/oversight/ttbr/sequoia-source-public-jul26.pdf

[6] California Secretary of State Debra Bowen's Report to the Election Assistance Commission Concerning Errors and Deficiencies in Diebold/Premier GEMS Version 1.18.19 (2009). URL: https://www.sos.ca.gov/voting-systems/vendors/premier/sos-humboldt-report-to-eac-03-02-09.pdf

[7] SF RCV BDProcedures2009-Final.xls, obtained from San Francisco Department of Elections.

There is no formal written procedure for escalating the audit or challenging the election results based on such a discrepancy.

Finding 3. The current post-election audit procedure is not a risk-limiting audit.

Auditing Procedures for Non-RCV Contests

For a regular contest, the manual count produces a tally of the number of votes for each candidate. These numbers are then compared directly to the vote counts on the machine report for the precinct. The counting process is quite fast, because the ballots are first sorted into piles (one pile for each candidate), and then each pile is counted. We watched a video of the manual tally for a ballot measure; a member of the team counted the "Yes" pile, speaking "Yes, yes, yes, yes, yes…" at a rate of about two ballots per second.

If this manual tally process were carried out for every precinct, it would give assurance that the counts are correct in every precinct, and thus the totals are correct for the entire election, and thus the outcomes (winners) are also correct. Performing this process for a randomly selected fraction of the precincts therefore assures the outcome with some probability.

Auditing Procedures for RCV Contests

For an RCV contest, the team manually counts the first choices, second choices, and third choices separately, as if they were three independent contests, resulting in three counts for each candidate. These are compared directly to the machine report, which also provides vote counts of each RCV contest as though it were three independent contests. Next, the team carries out the RCV elimination process *at the precinct level*. That is, if no candidate has a simple majority of the first-choice votes *in the precinct,* then the candidate with the lowest number of first-choice votes *in the precinct* is eliminated, those ballots are transferred to piles for their second-choice candidates, and so on.

Since the actual election outcome is determined by elimination based on totals for the entire election, the sequence of candidates eliminated during the manual precinct tally bears no relationship to the actual elimination sequence. Also, checking the three independent totals does not verify the outcome, because the outcome depends on which first-choice votes are cast with which second-choice votes, not just how many of each there are. Thus the RCV manual tally process does not verify the outcome of the election (see Appendix A for a detailed example).

Finding 4. The manual tally procedure for RCV contests is significantly more complex than the procedure for non-RCV contests.

Finding 5. The manual tally procedure does not verify the outcome of RCV contests.

Alternative auditing procedures

The deletion of 197 ballots in Humboldt County led to the certification of incorrect results in the November 4, 2008, General Election. The discrepancy went undetected until it was discovered by an audit conducted by the Humboldt County Election Transparency Project. The ballots were scanned with a general-purpose, high-speed office scanner.[6] A pre-imprinter attached to the scanner printed a unique serial number on each ballot before scanning. The resulting scanned images were then counted by open-source image analysis software.

> **Finding 6.** Audits have been successfully conducted by scanning and counting ballots using ordinary office equipment and free software, and such audits can be effective at detecting errors in election results.

Joseph Hall et al. conducted risk-limiting audits of four contests in 2008, which took place in Marin, Yolo, and Santa Cruz Counties, and reported that "[t]he cost and the time required were modest. … There remains room for big gains in efficiency—that is, for reducing the number of ballots that must be counted to confirm an election outcome that is, in fact, correct."[8]

> **Finding 7.** Risk-limiting audits have been carried out successfully in California.

Those who conducted these risk-limiting audits also reported that "[a] great deal of scripting and hand editing was required to make the exported data [from Election Management Systems] useful. … Election auditing requires better 'data plumbing' than EMS vendors currently provide. … One suitable format is the OASIS Election Markup Language (EML)…."[8]

Neal McBurnett worked with the Boulder County Elections Division to conduct an audit for the 2008 General Election in Boulder County, Colorado[9], and found:

- Most of the reports produced by the Hart tally system were poorly specified or hard to parse for auditing.
- The Hart tally system produced an XML report that was usable for auditing, though it still lacked some important information and did not adhere to the EML standard.
- Effective audits are easier and require less hand-counting to achieve a similar level of confidence if results are reported in smaller audit units.

Both of these reports point to non-proprietary reporting formats, specifically EML. We are also aware of IEEE P-1622, another voting data standard under development, with more of a focus on elections in the United States. We have not reviewed the specification for P-1622, as the group's working documents are not freely available. If and when P-1622 is a fully developed, freely available open standard with comparable expressiveness to EML, it may also be a suitable option.

[8] Joseph Lorenzo Hall, Luke W. Miratrix, Philip B. Stark, Melvin Briones, Elaine Ginnold, Freddy Oakley, Martin Peaden, Gail Pellerin, Tom Stanionis, Tricia Webber (2009). Implementing Risk-Limiting Post-Election Audits in California. URL: http://www.usenix.org/event/evtwote09/tech/full_papers/hall.pdf

[9] Neal McBurnett (2008). Obtaining Batch Reports for Audits from Election Management Systems: ElectionAudits and the Boulder 2008 Election. URL: http://www.nist.gov/itl/vote/upload/neal-mcburnett-boulder-paper.pdf

Finding 8. The use of proprietary, vendor-specific data formats increases the difficulty of conducting an audit or forensic investigation.

Finding 9. Election Markup Language is a suitable structured data format for enabling efficient post-election audits.

As McBurnett and others have found, using smaller audit units reduces the number of ballots that need to be verified by hand in order to achieve a high level of confidence. Calandrino, Halderman, and Felten[10] have proposed an auditing method with the smallest possible audit unit: each ballot is an audit unit. This method requires machine assistance to mark each ballot with a unique number so that individual randomly selected ballots can be retrieved and checked against their corresponding cast vote records. The number of ballots to check depends on the margin of victory; closer contests require more manual checking. Calandrino et al. analyzed the statewide contests in the Virginia elections in November 2006, and found that achieving a 99% confidence level with a post-election audit would require the hand counting of 40 times fewer ballots using their individual-ballot method, as compared to precinct-based auditing.

Finding 10. As compared to the current practice of auditing the tallies of randomly selected precincts, audits of individual randomly selected ballots can provide stronger confidence with greatly reduced manual counting effort.

Finally, we note that California Assembly Bill 2023 authorizes the establishment of a groundbreaking pilot program to conduct risk-limiting audits in "5 or more voluntarily participating counties" during 2011. The program will yield a report to the California Legislature evaluating the effectiveness and efficiency of the audits. We find that the definition of "risk-limiting audit" given in AB 2023 matches the meaning intended in this report.

Finding 11. The AB 2023 pilot program provides a valuable opportunity to conduct officially recognized risk-limiting audits and contribute to advancing the state of the art in post-election auditing procedures.

Recommendations

Based on the findings above, the VSTF makes the following recommendations. Recommendations 1 through 6 can begin implementation now. Recommendations 7 through 11 concern longer-term or more speculative changes, such as the criteria for San Francisco's next voting system. Below, the phrase "EML or an equivalent open standard" refers to a publicly

[10] Joseph A. Calandrino, J. Alex Halderman, Edward W. Felten (2007). Machine-Assisted Election Auditing. URL: http://www.usenix.org/events/evt07/tech/full_papers/calandrino/calandrino.pdf

available, freely licensed format of equivalent expressiveness to EML, established by a vendor-independent national or international technical standards body.

Near-term recommendations

1-Publish all election records on the city's website, redacting records only as necessary to protect the anonymity of each voter's votes and the privacy of each voter's personally identifying information. Give public notice when records are published. Whenever feasible, use EML or an equivalent open standard format for the published records. The VSTF recommends prioritizing these four types of records first:

A-Tallies of the results from each precinct: Publish (using EML section 500 or equivalent formats) as soon as possible after each precinct closes its polls.

B-Text files of cast ballot records, which are currently called "ballot image files": For precinct-scanned ballots, publish as soon as the memory packs are loaded; for centrally scanned ballots, publish as soon as the ballots are centrally scanned. These must be published before any precincts are randomly selected for audits.

C-Election definitions: Publish (using EML section 200 and 600 or equivalent formats) as soon as the Qualified Candidate List and Official Measures List are complete.

D-Ballot definition files: Publish (in the current proprietary format) as soon as ballot layouts are complete. When EML or an equivalent open standard format is used (see recommendation 7), publish EML.

2-Define and use risk-limiting audit procedures for all non-RCV contests, taking guidance from "Implementing Post-Election Audits in California" [8]

3-Correct the audit procedure for RCV contests in such a way that a 100% tally would actually ascertain the outcome. In particular, as recommended by the California Secretary of State, use entire-election totals, not precinct vote totals, to determine which candidates to eliminate[11].

4-Permit academic organizations to publicly request and obtain timely access to the paper ballots for the sole purpose of digitally scanning the ballots and analyzing the scanned images to independently verify election results, and to publish their findings from such verification.

5-Permit academic organizations to publicly request, obtain, and study machine audit logs from which information identifying individual voters has been removed, and to publish their findings from such study.

6-Pursue participation in the post-canvass risk-limiting audit pilot program authorized by California AB 2023.

[11] Debra Bowen. Instant Runoff Voting Guidelines. URL: http://www.sos.ca.gov/voting-systems/oversight/directives/irv-guidelines.pdf

Longer-term recommendations

7-Consider broadening the audience with access in recommendations 4 and 5 to include other organizations that serve the public interest, or all members of the public, under conditions that limit conflicts of interest, protect voter privacy, and discourage vote-selling.

8-Use EML or an equivalent open standard format internally within the Department of Elections as the primary data format for election definitions and results.

9-Announce an acquisition preference for voting systems that enable auditing of individual randomly selected ballots, for example, by printing a unique identifier on each ballot to associate it with the digital cast vote record for that ballot.

10-Consider stating support for EML or an equivalent open standard format as a procurement requirement for new voting systems—specifically, as the format for election definitions, results, outcomes, and any reports necessary to support the risk-limiting audit procedure in use.

11-Announce an acquisition preference for voting systems that allow individual voters to verify their cast votes after the election and independently check the vote tally.

12-Pursue the implementation of risk-limiting audit procedures for RCV contests as soon as viable methods have been established in the research community.

Balloting Systems & Services

Introduction

This section addresses selected issues and opportunities for balloting systems and services, which the Voting Systems Task Force believes are the most important to consider in any next-generation elections administration and voting systems platform. Where possible, this section makes tactical recommendations that can be applied to the current system(s) in place. However, the majority of this material focuses on recommendations to guide the defining of requirements and specifications for any future voting system acquisition to enhance, extend, or replace what the City and County of San Francisco currently has deployed.

Concepts and Definitions

- **Ballot Marking Device (BMD)**: Refers to a computer based device that: presents a ballot as a series of ballot items; accepts voter selection(s) for each ballot item; provides navigation, help, confirmation and other UI functions; records the voter's selections by printing a paper ballot that the voter can cast in the same manner as paper ballots that were marked by hand. Some BMDs print only selection marks (e.g. bubbles) on pre-printed ballots; other BMDs print a complete ballot on a blank sheet(s) of paper.

- **Balloting Systems and Services**: As the ~~phase~~ is used in this Report and titles this subsection, refers to those technologies employed for the following uses of secret ballots in a public election: producing ballots prior to an election, or on-demand during an election; delivering a ballot to a voter, either in person, or remotely for absentee voters; marking a ballot, whether manually marking a paper ballot, or digitally marking an electronic ballot, or using digital means to indicate ballot choices that are then represented on a printed ballot; presenting a ballot to be counted, whether remotely or in-person, or presented physically or digitally; and the actual counting of ballots.

- **Central Count Optical Scan Device (CCOS)**: Refers to a computer based device that incorporates digital image capture and digital image processing techniques to acquire an image of each sheet of a deck of paper ballots, identify voter marks on the ballot, and interpret each mark as a choice for a particular contest's candidate or choice. The votes from each scanned and counted ballot are tallied to produce vote totals from the set of ballots scanned during a single run of the device. Some CCOS devices retain ballot images and/or individual records of each counted ballot. Some CCOS devices reject ballots with ambiguous marks, while others provide a user interface for election officials to interpret the voter's intent and indicate how an ambiguous mark should be realized and recorded as a vote or non-vote.

- **Direct Recording Electronic Device (DRE)**: Refers to a computer based device that: presents either a fullface ballot or a series of individual contests or races on an electronic screen; accepts voter selection(s); provides navigation, help, confirmation and other UI functions; records an electronic ballot that comprises all of a voter's ballot selections.

Some DREs include a printer that produces a physical copy of the ballot selections or a Voter Verified Paper Audit Trail (VVPAT).

- **DRE Double Commit**: Refers to a DRE function that creates a risk for disenfranchisement. With some DREs, when a voter casts a ballot, the voter is prompted to confirm that they are finished voting, and then prompted a second time to commit and cast the electronic ballot. The disenfranchisement risk arises in practice because voters sometimes leave the polling place after the first confirmation, but without responding to the prompt for the second confirmation. At that point, the DRE will eventually time-out the voter session and not cast or count the ballot; also, until that time, poll workers have the opportunity to cast the ballot, either as is, or with modifications to the voter's selections.
- **Federal Election Assistance Commission (EAC)**: An agency of the U.S. Federal government, created by the Help America Vote Act (HAVA) of 2002, tasked with assisting state and local election administration organizations in improving their capability to conduct U.S. government elections. The EAC primarily funds state and local election administration organizations, but also awards research contracts for investigation of election-related matters. The EAC has funded the replacement of voting systems for much of the country, notably including voting systems that meet HAVA mandates for accessibility.
- **Federal Write-In Absentee Ballot (FWAB)**: A paper form that UOCAVA voters may use when their regular ballot has not been received, even though they made a timely application for their ballot. The voter fills out the absentee voter affidavit, and writes a list of contests/candidates and the voter's choice for each one. This requires that the voter have independent and accurate knowledge of the contests/candidates that the voter is qualified to vote on. Inaccuracies on the voter's part in filling out the form, combined with vote-by-mail anonymity protections, may result in a voter voting for an item that they are not qualified to vote on. In practice, many FWABs are not counted or not fully counted because of errors or omissions in the affidavit or the contest/candidate list.
- **Precinct Count Optical Scan Device (PCOS)**: Refers to a computer based device similar to a CCOS device, except that a PCOS device scans individual paper ballots one at a time rather than a deck of ballots. Can be set to reject ballots with contests/races that are undervoted/overvoted, thereby giving the voter an opportunity to make a selection for an undervoted ballot item or to obtain a new ballot for an overvoted ballot item.
- **Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)**: An act of the U.S. Congress that places requirements on states' conduct of elections to include measures to enhance access by military or civilian voters not residing in the U.S., or by military voters on service away from their locality of voter registration.
- **Vote By Mail (VBM)**: A voting method by which a blank ballot and voter affidavit are sent via postal service to an absentee voter, who is expected to complete both documents and return them via postal or express service, packaged in such a way that the affidavit can be viewed without viewing the marked ballot. Jurisdictions employ a wide variety of methods for packaging, for information required on affidavits, and for validation, if any, of the affidavit sometimes including a signature.

- **Voter-Verified Paper Audit Trail (VVPAT)**: Refers to a paper-based component of a DRE. Some DREs print a VVPAT for a voter to review and independently verify their ballot selections before casting an electronic ballot. Such VVPATs are automatically put into a secure container after the voter has finished voting. In some jurisdictions, VVPATs are used for hand-count audits of DRE counts. Depending on state law, the VVPAT may or may not be considered the official record of a vote.

1. Ballot Accessibility and Availability

1.1. Findings

1.1.1. The current state of ballot accessibility and availability issues apply distinctly to three (3) categories of voters:

1.1.1.1. **Local In-person Voter**:

1.1.1.1.1. Voter and Ballot information is provided by postal distribution and Web publication of personalized sample ballots that are close facsimiles of the actual paper ballots.

1.1.1.2. **Uniformed and Overseas Voter**:

1.1.1.2.1. Voter and Ballot information as well as the official vote-by-mail blank ballot with an associated attestation document are made available by postal distribution at least, and digital means at best to be compliant with Federal MOVE (Military and Overseas Empowerment Act of 2009) Act regulations.

1.1.1.3. **Other Absentee Voters**:

1.1.1.3.1. Voter and Ballot information as well as the official vote-by-mail blank ballot with an associated attestation document are provided by postal distribution.

1.1.1.3.2. Applications materials for absentee voter status are available by Web download for preparation and return via postal service or in-person delivery.

1.1.1.3.3. Special needs voters are able to obtain assistance in ballot marking and casting only if they are physically able to make it to a public polling place. These voters' only option is to rely on paper vote-by-mail ballot if they are able.

1.1.2. In addition to these findings, there are issues pertaining to accessibility and usability of the ballot itself.

1.1.2.1. **DRE devices with VVPAT for disabled voter ballot casting**

1.1.2.1.1. These devices do not produce a durable paper ballot of record equivalent to ballots provided to non-DRE voters.

1.1.2.1.2. For special-needs voters utilizing DRE-based ballot casting services there is an increased risk of loss of anonymity[12].

1.1.2.1.3. DRE-voters are disadvantaged in audits or recounts due to the less durable nature of a VVPAT ballot compared to standard paper ballots

1.1.2.1.4. VVPAT rolls of paper are difficult to count in the case of manual recounts and full recounts.[13]

1.1.2.2. **Paper ballot usability limitations**

1.1.2.2.1. The need exists to verify that instruction text meets EAC guidelines for plain-language and moderate-level literacy accessibility.

1.1.2.2.2. The need exists to verify visual aids exist in instruction text.

1.1.2.2.3. There is likelihood that Ballot layout does not meet guidelines of EAC-funded AIGA best practices in ballot design[14].

1.2. Short-Term Recommendations

1.2.1. Support provisions of federal MOVE Act regulations[cite] for digital blank ballot distribution.

1.2.2. For special-needs San Francisco based voters who are physically unable to cast their ballot in a polling place, experiment with mobile accessible ballot marking and printing services.

1.2.3. Promote the opportunity for San Francisco voters to access voting information online, including sample ballots.

1.3. Long-Term Recommendations

1.3.1. Extend the intent of the CA Election Code Section 15360 by requiring the ballot of record to be more than a mere paper artifact fulfilled by VVPAT devices, but specifically a paper record of uniform style, layout, and presentation consistent with its hand-marked counterpart.

1.3.2. Use paper ballot layout practices and/or tools that follow the EAC guidelines on visual design and plain language, and deliver these benefits to all voters.

[12] The risk of non-anonymity deserves comment. If a few hundred people in a polling place vote on paper and PCOS, and a handful of special-needs voters use a DRE, then poll workers know that the handful of special-needs voters cast that handful of votes. In a primary, if only one voter of that handful was registered as say for example, a Green party voter, then poll workers would know exactly who cast that single (for instance) Green Party ballot on the DRE.

[13] For example, image in middle of this page: http://www.countedascast.com/issues/audits.php

[14] See generally: http://www.aiga.org/content.cfm/election-project

1.3.3. Rather than polling-place disabled access via DREs, instead provide access via ballot-marking devices, that lack the so-called “*double-commit issue*,” that provide for a digital count for audit purposes, and that follow the EAC guidelines on visual design and plain language.

1.4. Rationale

The following itemized rationale is intended to support the foregoing recommendations.

1.4.1. **MOVE Act Support**. The State of California historically asserted compliance to the MOVE Act 45-day advance availability provision by postal distribution means of absentee voter materials for UOCAVA voters. Nevertheless, exploring opportunities to make these materials more readily available by digital means pursuant to the MOVE Act could better serve our overseas and military voters.

1.4.2. **Mobile Accessible Balloting Services**. Special needs voters tend to be disenfranchised should their individual situation prevent their ability to travel to a polling place to cast their ballot.

1.4.3. **Ballot Design and Paper Ballot of Record**. As an equal protection principle, consistent enfranchisement depends on consistent ballot format and ballot counting procedures. This principle is not currently met in practice because some voters have their votes counted from paper ballots, while other voters have their the votes counted relying on VVPAT devices. Therefore, aspiring to a single ballot design, layout, and presentation for the ballot of record can achieve the long-term recommendation.

1.4.4. **Ballot Marking Device**. This longer-term undertaking is intended to support the uniform paper ballot of record recommendation by utilizing a marking device rather than a DRE, which will produce a paper ballot for counting, audit, and verification purposes.

2. Ballot Marking and Casting

2.1. Findings

2.1.1. The current state of ballot marking and casting can be divided into two areas: in-person voting and remote voting.

2.1.1.1. **Remote Voting**: It is well settled that marking ballots in an uncontrolled environment is vulnerable to fraud, and there is significant controversy regarding the security risks of any remote digital voting.

A notable exception to the foregoing was the Okaloosa Distance Balloting Pilot, which used a combination of early-voting center operations, kiosk-style Internet voting in controlled environment, and paper ballot-like voter-verified paper records used for auditing the Internet voting tallies.More recent proposals for digital-enabled kiosk voting have included methods that do not rely on Internet voting techniques. In any event, the concepts of controlled environment and a verifiable paper trail and audit trails have emerged as the top issues wherein any remote voting solution is contemplated. Citations: http://www.operationbravo.org/documents/NASS%20VP%20Briefing.pdf AND http://election.dos.state.fl.us/voting-systems/pdf/ODBPplanJune_19.pdf

2.1.1.2. **In-Person Voting**: Casting and counting of ballots in person in polling places uses two methods: precinct optical scan of hand marked ballots, and use of DRE devices for digital casting and counting.

2.1.1.2.1. In addition to the foregoing methods, some voters are required to vote provisionally by casting a hand-marked paper ballot that is not counted in the polling place but may be counted centrally, if approved by election officials.

2.1.1.2.2. San Francisco also employs central count optical scan for vote-by-mail ballots and provisional ballots that have been approved by elections officials.

2.1.1.2.3. A third type of ballot is the Federal Write-In Absentee Ballot (FWAB), which is approved by a process similar to vote-by-mail process, but requires manual intervention for counting purposes.

2.2. Long-Term Recommendations

2.2.1. The official "ballot of record" should be a paper artifact in uniform design, layout, and presentation consistent with its hand-marked counterpart (see also 1.4.3 above), in order to enable a consistent method of counting, audit, and verification, as well as to ensure a consistent method of ballot anonymity.

2.2.2. Enhanced access to ballots should be provided by non-tabulating ballot marking devices rather than tabulating DREs.

2.2.3. All in-person voters should have the options of either marking paper ballots by hand, or via the use of a BMD (ballot-marking device)[15].

2.2.4. Encourage voters who use BMDs to review their printed ballots before casting.

2.2.5. All optical scanning devices should retain a good-resolution scanned image of each ballot, together with a complete cast-vote record for auditing support.

2.2.6. CCOS devices should provide a user interface for election officials to interpret ambiguous ballot marks as needed, with full logging of every interpretation, said logs to be publicly available.

2.2.7. If not done so already, provide data to track cases of UOCAVA voters receiving absentee voting materials, but not having a ballot arrive in time to be counted.

2.3. Rationale

The following itemized rationale is intended to support the foregoing recommendations

2.3.1. **Single Ballot Type**. Equal protection and enfranchisement is supported by a single kind of ballot and a single method of counting, which can be supported along with support for accessibility.

2.3.2. **Ballot Marking Device**. BMDs ensure two principles: [**a**] special-needs voters obtain automated assistance in ballot marking; and [**b**] all voters have a paper ballot that is consistently counted in the same manner

2.3.3. **Ballot Image Retention**. Provides for improved audit and verification.

2.3.4. **CCOS Logging Capability**. Provides for improved accountability, audit, and verification.

[15] In California, the voters do have the choice of using paper ballots or DREs with VVPATS. However, as a policy matter, the use of DREs is discouraged, since all votes cast on a DRE with VVPAT must be counted by hand.

Security

Background

Elections security is important to protect voter rights and assure the integrity of election data. Security throughout the election cycle, including use of the voting systems, is implemented with procedures. Security of voting system itself is fundamental to the system design, engineering and manufacture and is every bit as important as procedural implementation of security to our assurance of the integrity of our election results.

When considering voting system security, we need to examine the vulnerabilities throughout its use in the election cycle. The following are major parts of the end-to-end election process for the voting system:

Ballot Definition: Paper and electronic descriptions of the contents and layout of each type of blank ballot.

Vote Capture: This is the point at which a vote becomes a cast vote record (CVR), which will ultimately be aggregated with other votes to determine the election result. For paper ballots, the precinct or central ballot optical scanner device (Sequoia Eagle and 400C respectively) translates the marked, paper ballot to a digital record of the vote. When a “direct recording electronic” device (Sequoia Edge DRE) is used , the digital vote record is created by touching the device’s screen to cast a vote. The DRE also produces the Voter Verifiable Paper Audit Trail (VVPAT). Note that in advance of use for an election the law requires that all machines undergo a logic and accuracy (L&A) test. They may be recalibrated or repaired as needed to assure they are fit for use in the election.

Vote Transmission: This involves moving the electronic data to an electronic/digital database all votes for San Francisco can be read by a computer that tabulates the election results. Data can be “sneaker netted” (downloading data to a device which is transported to another location and uploaded to another location) or may be transmitted electronically over a network. In San Francisco, the data recorded by the precinct optical scanner and the precinct DRE (Sequoia Eagle and Edge respectively) is saved to a removable memory pack that is transported from the precinct to the election center for upload to the central election database. Vote by Mail Ballots are received at the election center and counted by large, fast optical scanning machines (Sequoia 400C) which transmit data to the central data store over a private computer/data network of CCSF.

Vote Tabulation: At this step, votes are tallied to determine the result for each election contest. For contests that are determined by a plurality, this is a matter of summing of the votes to determine passage of a measure or winner of a race. For RCV, when there is no one candidate who received 50% +1 vote in the first count of an RCV race, computer algorithms to eliminate candidates and redistribute votes when needed the voter's second or third choice candidate.

Our reliance on voting systems in the election process means that we must takes steps that build trust that the digital chain of custody has not been broken nor that any event has occurred that might affect the integrity of the election data. For physical ballots and for the voting system , there are opportunities for fraud or error. The difference between the physical ballots and electronic version of the ballot data it is that without proper system security the opportunities for fraud and error can be much greater in volume and more precise in their intended impact and be harder to detect. Thus, security in our voting systems is essential to trusting the election outcome and we must continue to use procedural measures to both bolster security and to detect issues such as fraud or error. A system that is designed with security taken into consideration across its elements – hardware, software, firmware, data, network – will improve our confidence in the system and can reduce the cost of the procedural methods of security assurance.

The focus of voting system security is on preventing events which cause corrupt or inaccurate voting data or otherwise disrupt the ability to obtain an accurate election result from the voting system whether the cause was malicious or an innocent mistake. As discussed, we cannot rely solely on preventive security measures because we cannot make a perfectly invulnerable system. Thus, we must include the review and audit of the voting system, as a means to detection of possible fraud or error, to provide the assurance that security measures were successful or that no system events, unauthorized or improper access might compromise the system or the election data. Only with this detective step is the security regimen complete.

- **San Francisco's Current Voting System: Existing Security Issues and Mitigation**

1.1 San Francisco's Procurement Action and Voting System Security Concerns

In May of 2005, San Francisco issued a Request For Proposal (RFP) for procurement of a voting system. The RFP's Appendix E Design, Fabriction and Performance Requirements contains the the security specifications for the system to be procured. Security is mentioned 13 times and \ the section devoted to security is168 words in length[16]. The RFP demonstrates interest by the Dept of Elections (DOE) in voting system security, but the requirements are not in depth, do not

[16] City and County of San Francisco Department of Elections Request of Proposals for a New Voting System RFP# NVS0305, Appendix E Section 3.4, page E-22

require the bidder to disclose security of ~~it's~~ designs. This reflected the reality of the voting system circumstances at that time which included reliance on existing Federal certifications and requirements to procure a new system. San Francisco needed to replace a system that was aging and for which the maintenance contract was about to expire. The Federal government, through the Help America Vote Act (HAVA), had mandated a modernization of voting systems and funds were provided for implementation of this mandate.

The systems that could be implemented to satisfy HAVA requirements and were certified for both Federal and California elections were few. Only 2 of those vendors responded to the San Francisco's RFP. Despite public objections primarily due to transparency and security concerns, -- which stalled execution of the contract for 15 months, -- and due to the fact there were no viable alternative, certified voting systems available, San Francisco proceeded with the procurement. From the standpoint of the SF Department of Elections, proceeding with the procurement was the prudent course of action. This would bring the Department into compliance with Federal law and serve its operational needs so any additional consideration of security was unnecessary and superfluous to fulfillment of its legal obligations and operational mission.

Thus, San Francisco would be in compliance and the DOE would be operationally served by a newer voting system, so any additional consideration of security was unnecessary to fulfill its legal obligations and organizational mission.

In January 2007, Debra Bowen was sworn in as the California Secretary of State and reiterated her campaign promise to test the voting systems used in California. Her office contracted with the Regents of the University of California to employ a team computer scientists and other experts from the University of California to conduct a Top To Bottom Review (TTBR) of the voting systems certified for use in California, including the Sequoia system procured by San Francisco. The review team found many serious security issues in all of the systems they examined. The TTBR homepage[17] states that "The reviewers were responsible for analyzing voting system security, accessibility, usability, reliability, accuracy and protection of ballot secrecy based on relevant documentation."

The following is an excerpt of the of the Executive Summary of the TTBR "Source Code Review of the Sequoia Voting System"[18]

> "_ **Data Integrity.** The Sequoia system lacks effective safeguards against corrupted or malicious data injected onto removable media, especially for devices entrusted to poll

[17] Top to Bottom Review, http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm

[18] Source Code Review of the Sequoia Voting System, July 20 2007, page 2 http://www.sos.ca.gov/voting-systems/oversight/ttbr/sequoia-source-public-jul26.pdf

workers and other temporary staff with limited authority. This lack of input validation has potentially serious consequences…”

“_ **Cryptography.** Many of the security features of the Sequoia system, particularly those that protect the integrity of precinct results, employ cryptography. Unfortunately, in every case we examined the cryptography is easily circumvented. Many cryptographic functions are implemented incorrectly, based on weak algorithms with known flaws, or used in an ineffective or insecure manner. Of particular concern is the fact that virtually all cryptographic key material is permanently hardcoded in the system (and is apparently identical in all Sequoia hardware shipped to different jurisdictions). This means that an individual who gains temporary access to similar hardware (inside California or elsewhere)

can extract and obtain the secret cryptographic keys that protect elections in every California county that uses the system.”

“_ **Access Control.** The access control and other computer security mechanisms that protect against unauthorized use of central vote counting computers and polling place equipment are easily circumvented. In particular, the security features and audit logs in the WinEDS back-end system (used for ballot preparation, voting machine configuration, absentee ballot processing, and post-election vote counting) are largely ineffective against tampering by insider attackers who gain access to WinEDS computers or to the network to which the WinEDS computers are attached.”

“_ **Software Engineering.** The software suffers from numerous programming errors, many of which have a high potential to introduce or exacerbate security weaknesses. These include buffer overflows, format string vulnerabilities, and type mismatch errors. In general, the software does not reflect defensive software engineering practices normally associated with high-assurance critical systems. There are many instances of poor or absent error and exception handling, and several cases where the software behavior does not match the comments and documentation. Some of these problems lead to potentially exploitable vulnerabilities that we identified, but even where there may not be an obvious vulnerability identified, the presence of such errors reduces our overall confidence in the soundness of the system as a whole.”

INSERT SEQUOIA In the examination of the Sequoia voting system the TTBR Computer Security Group, which “…acted as a Red Team and performed a series of security test of both the hardware and the software” concluded in its Public Report that[19]:

[19] Security Evaluation of the Sequoia Voting System Public Report, 2007, page 12 http://www.sos.ca.gov/voting-systems/oversight/ttbr/red-sequoia.pdf

> "Although, we did not have enough time to perform a complete evaluation of the Sequoia voting system, we exposed a number of serious security issues. These vulnerabilities could be exploited by a determined attacker to modify (or invalidate) the results of an election.
>
> All the attacks described in this report can be carried out without any knowledge of the source code. In fact, we were able to extract and analyze the Edge's firmware binary representation. In addition, we were able to extend the firmware by using binary patching. This technique allowed us to create a "debugging" version of the firmware, as well as several different "malicious" versions.
>
> The implementation of the attacks did not require access to the source code."

1.2 Security Mitigations Measures Required to use the Sequoia Voting System

As a result of the reports by the TTBR team, Secretary of State Bowen issued the "WITHDRAWAL OF APPROVAL OF SEQUOIA VOTING SYSTEMS, INC."[20] which also included the requirements for reapproval of the system. The result was generation of the "Optech Insight, AVC Edge 5.0, & Optech 400C California Procedures" [21] deemed the "Sequoia 4.0 Approved Use Procedures" which allowed conditional reapproval of the system and, with implementation of these procedures, the use of the system in San Francisco.

Thus, public concern over security issues of the Sequoia voting system San Francisco was to procure was not unfounded. At this time, however, San Francisco and Sequoia have implemented the mitigation plans approved by the Secretary of State, who continues to monitor the vendor's on-going mitigations and their implementation by San Francisco. Thus, the VSTF makes no further recommendations for extending security on the current Sequoia system. However, the public interest would be served by raising awareness of the Sequoia system vulnerabilities discovered in the TTBR, the mitigation measures prescribed by the CA SoS Secretary of State and the procedures that implement these measures in the City and County of San Francisco.

1.3 Recommendation

Accordingly, this Report recommends There is a need for increased transparency, communication and education of the public about San Francisco's implementation of the

[20] WITHDRAWAL OF APPROVAL OF SEQUOIA VOTING SYSTEMS, INC., …" http://www.sos.ca.gov/voting-systems/vendors/sequoia/sequoia-31012-revision-1209.pdf

[21] Optech Insight, AVC Edge 5.0, & Optech 400C California Procedures, 8/2008 http://www.sos.ca.gov/voting-systems/vendors/use-procedures/sequoia-use-procedures.pdf

Secretary of State-mandated mitigations. Specifically, the City should create an online resource to complement voter information resources that describes the current system, features, and functions, complete with a walk-through of the steps taken to comply with the SoS Secretary of State reapproval mandates for the current voting system.

2. Near to Medium Term: Steps in the Interim Towards Future Systems

Beyond the immediate security concerns specific to San Francisco's current voting system, there are also broader concerns about information security of voting systems. The VSTF's recommendation for the short to medium term is that San Francisco should increase (a) public awareness and education on the security posture of computer-based vote counting, and (b) transparency of operations with regard to this posture.

2.1 Security of San Francisco's Current Voting System

Regarding SF's San Francisco's existing counting methods, based on optical scanning of paper ballots, the fundamental security posture consists of (1) implementing best practices and legal requirements for security and (2) validation of machine counts by conducting partial hand-counts of 1% of the precincts, or a one percent manual tally, as required by California Elections Code Section 15360. The security practices and requirements include reducing or eliminating exposure to attack points such as connections to wireless devices or the Internet, and using tamper-evident seals, signature checks, and other chain-of-custody procedures that increase the chances of detecting errors or tampering;. . "Technology independent" validation as the phrase applies in this Section of the Report means that vote counts and election results are **not** produced by the sole reliance on the fallible software and hardware of a voting system, but instead are produced by a combination of:

1. Machine count of virtually 100 percent[22] of paper ballots
2. Audit of the machine counts via hand-count of a randomly selected subset of the machine-counted ballots.[23]

The audit procedure is intended to detect discrepancies in the vote count as tabulated by the voting system versus a hand count of the ballot of record. This procedure should audit a statistically significant sample relative to the number of races and voters, and should provide a threshold to expand the scope of the audit in the event that significant variances are detected.

As already discussed with respect to security, the audit approach is a forensic method for **detection** of error and could only discover exploitation of security vulnerabilities with secondary

[22] Federal Write-in Absentee Ballots or "FWAB", if cast, must be hand counted

[23] Precinct cast ballots on Sequoia Edge Direct Recording Electronic (aka DRE) device do not produce a paper record that is machine read. Instead, the vote data is recorded directly to the memory pack that is then transported to a central location and loaded into the main tabulator along with the memory pack from the Sequoia Eagle Optical Scan device. The DRE does produce a paper tape record of the voter's selection by contest (Voter Verified Paper Audit Trail, aka VVPAT). This paper tape record can be used for audit purposes.

investigation. **Prevention** of errors by exploitation of security vulnerabilities means seeking to create a secure or trustworthy system. It is well settled that a perfectly secure system is an impossible goal because all software is potentially fallible.

That observed, it is also important to note that basic, prudent security measures are already in practice including but not limited to:

- Keeping voting systems components disconnected from public networks; and
- Checking the integrity of device firmware and/or software on voting systems components through pre-election logic and accuracy tests

2.1 Recommendations

Many such basic measures are specified as TTBR mitigations, logic and accuracy testing practice, and post-election operations reviews. With that in mind, the VSTF recommends the following actions be taken until any future system can be acquired:

1. The City and County of San Francisco should endeavor to increase public trust by increased communication of:
   - 1.1. The basic points of the security posture summarized above, and in particular that:
     - 1.1.1. Perfectly secure voting system software is impossible;
     - 1.1.2. Manual audits remove the need to trust in the correctness and integrity of software.
   - 1.2. The existing practices of L&A testing and TTBR mitigation
2. Increase the operational transparency and adequacy thresholds of statistical audit practices, including
   - 2.1. Greater information on and availability of audit results; voter education about auditing and results through online resources that complement existing voter information services.
   - 2.2. Consider various options for increasing the scope of audits beyond the minimum requirements of the California Elections Code. (see Post-Election Audit section of this report.)

3. Security for San Francisco's Future Voting Systems

3.1 Comprehensive Voting System Security Examination not attempted by VSTF

The VSTF did not attempt a comprehensive examination of information security as it applies to voting systems. The threefold reasoning became clear during the Task Force's work. First, voting technology experts concur that future voting systems design will require a wholesale change in the technology model, including testing and certification methods and requirements for Federal certification in order to increase accuracy, transparency, verification, security, and above all, trust. the Second, the prospective 4th version of the NIST/US EAC Voluntary Voting System Guidelines (VVSG) containing the most extensive set of specifications and procedures for security yet developed, was expected to be released in 2009, but remains unadopted in a final form. Third, the state of the voting systems industry is bleak. Two major vendors control 87% of US voting systems in use, with a few smaller vendors serving small pockets of opportunity. The VSTFs ability generate guidance on security that would meaningfully influence existing vendors was considered extremely limited. Therefore, the VSTF found with regard to voting systems security considerations, that a more focused study by more qualified security experts is necessary.

3.2 Principal Recommendation

The VSTF's overarching recommendation with regard to voting system security is that the City and County of San Francisco collaborate with or create a new, highly qualified, agile small team of computer systems scientists to develop a set of *guidelines* for security aspects of any future voting system to be acquired.

For a procured system, these guidelines should comprise new security requirements to be incorporated into any future Request for Proposal to be responded to by any provider of voting systems to the City and County of San Francisco. Should San Francisco proceed with a decision to make a system to their requirements, these guidelines should be further developed to become requirements that are incorporated into overall systems design.

This new Security Guidelines Team could be a new task force or simply collaboration with both academia and computer industry professionals on a consultative basis, who have demonstrated domain expertise in elections technology and related information security matters[24].

3.3 Forward-Looking Security Capabilities and Features

Lastly, aside from assembling a team of digital security experts to develop RFP guidelines for future voting systems, the VSTF suggests several features that can support increased voting systems security and elections process integrity, many of which are discussed elsewhere in this Report:

1. Assuring a system that allows for hand marking of paper ballots, machine-assisted creation of marked paper ballots (versus VVPAT) for voters with requirements for enhanced access;
2. Continued use of Precinct-count optical scan for in-person cast ballots and Central-count optical scan for absentee and provisional ballots;
3. Digital images of each counted ballot, with a cast-vote record for each for which are made available for examination

[24] By way of example, but not limitation three example sources of domain experts include: [**a**] the California Institute of Technology and Massachusetts Institute of Technology joint project known as the **CalTech/MIT Voting Project** (see: http://vote.caltech.edu/drupal/); [**b**] **ACCURATE** – A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections, the organization involved with the TTB Review (see: http://accurate-voting.org/); and [**c**] The **OSDV Foundation**'s **TrustTheVote Project** (see: http://www.osdv.org and http://www.trustthevote.org)

4. Logging of central-count operator actions including changes of votes, resolution of under-votes and over-votes, recording of write-ins, etc.;
5. Election management system features and reporting system features for publication of ballot definition data and vote count data as recorded by counting devices;
6. Use of common data formats to facilitate publication of such data; and
7. Features related to verification loops, testing practices, and transparency of records of such practices, including (but not limited to):
   7.1. Straightforward and easily repeatable measures for testing software integrity of voting system components;
   7.2. Election management system features and reporting system features for recording and publishing both components of and results of logic and accuracy testing (e.g., test decks and test count results)
8. A system that is well documented that can be maintained and operated with commonly and widely available skill sets (versus vendor-dependence due to proprietary elements and non-disclosure of system technology)
9. Strong protections to assure that only known actions with approved software or hardware implemented with documented, approved change management procedures are used during deployment or update of the system
10. Transparency throughout of system design, engineering and manufacture including hardware, software, firmware, data formats, encryption and communications protocols, and network security requirements
11. Voting system capabilties for strong authentication, access and event logging with notification and audit procedures that assure only authorized access and approved actions were taken in the system
12. Ability to validate only authorized software was used to execute the election in the system

Acquisition Strategies

Introduction

This section considers business and partnership models available to the City and County of San Francisco as it procures or develops its next voting system. It examines the related legal licensing options, including 1) proprietary, 2) disclosed, and 3) open source software and hardware approaches. It also puts forth software best practices that should be adopted regardless of the development strategy selected.

The choice of a business and partnership model, and the related licensing structure, is fundamental to transparency, and therefore has implications that reach across all topic areas addressed in this report. The VSTF advocates for transparency in all aspects of design, development, production and the business relationship of all parties associated with production, delivery, implementation, and use of the voting system. The goal is to achieve a cost effective, reliable, trustworthy, and maintainable system.

Definitions and Concepts

Public domain license: Refers to the class of license which is not limited by copyright and therefore essentially has no single owner to grant licenses. Since the work is not protected by copyright it can be used, modified, and distributed by anyone without limitation.

Open source software: The term open source software can refer to a range of concepts, such as software development practices, along with licensing rules. In this document we are using the Open Source Initiative (OSI) definition of open source software and are focused on licensing. See the definition the VSTF is using at http://opensource.org/docs/osd.

Disclosed source license: In this document, this term refers to a license that gives the licensee permission to review all source code, including that of firm-ware, and the ability to share all source code with other parties. All requestors should be able to run the code for testing purposes. No one should be restricted from publishing his/her findings. The code, however, can have a proprietary license, which would restrict some rights; for example, the copyright owners could require a fee to run the code in production.

Findings

Business and Partnership Models

"Voting system development and acquisition is driven primarily by a private vendor market. Most states and counties purchase/lease voting systems from commercial vendors. The contractual agreements in this model usually involve a lot of proprietary information that cannot be disclosed to the election officials or the public. In addition, most contracts – and current voting systems regulatory framework -- also place a number of restrictions on the ability of the election official to make modifications to the system, whether by agreement or by restricting access to proprietary source code.” ~ Los Angeles County Voting Systems Assessment Project Report dated July 9, 2010

The dominant model for implementing elections is for jurisdictions to purchase or lease proprietary voting systems from commercial vendors in the marketplace (see “A” below). While this is the prevailing course of action today, entirely new models for acquiring a voting system are beginning to be considered by some governmental and non-governmental organizations. Each possible approach brings a different set of economic and partnership considerations. A range of sample models includes:

A - Purchase a Commercially Available Voting System
A jurisdiction purchases a voting system (equipment and services) from a private vendor that funded its development and certification. The code is proprietary and owned by the vendor. The City and County of San Francisco employs this model with Sequoia Voting Systems.

B – Engineer to Order (Vendor Developed or Self-Developed)
A jurisdiction establishes system requirements and either uses an RFP process to select a vendor to build the voting system, or employs a full development team to build the voting system. In either case the jurisdiction owns the system. The voting system may be based on existing software components or may be built entirely from scratch. The jurisdiction funds the costs of development and certification.

C – Public Partnership
Jurisdictions with similar systems and regulatory requirements partner and share resources to build and maintain a voting system. The jurisdictions pool their resources to fund the costs of development and certification.

D – Public/Private Partnership
A jurisdiction seeks partners which may include academic institutions, non-profits, other government entities, or even private sector technology companies willing to produce non-proprietary components. Based on system requirements, the consortium develops the code and component parts. However, the code is not proprietary and the jurisdiction either owns the code outright or has the ability to make modifications. The potential funding for this model varies greatly depending on the specific solution, but usually will include a combination of money from jurisdictions and from donors/volunteers.

There are existing non-profits that are building open-source voting systems that are in various stages of readiness for elections. Two such organizations are the Open Voting Consortium (OVC) and Open Source Digital Voting Foundation (OSDV.) There are also myriad systems that have been built by individuals and groups at academic institutions. Although many were built for specific research purposes and aren’t made to be extended, some have the potential to be the basis for full voting systems. Some of the systems include Scantegrity and Helios. The Caltech/MIT Voting Technology Project is a good source of information on existing systems.

Certification

The following are requirements for a new voting system to be certified in California (see http://www.sos.ca.gov/voting-systems/cert-and-approval/vsysapproval/vs-conditions.htm)

- Review of the application and documentation of the system;
- End-to-end functional examination and testing of the system;
- Volume testing under election-like conditions of the system and/or all voting devices with which the voter directly interacts;
- Security testing that includes a full source code review and penetration (red-team) testing of the system;
- Accessibility examination and testing of the system; and
- Public hearing and public comment period.

Along with nine other states, the State of California also requires federal certification (http://www.sos.ca.gov/voting-systems/cert-and-approval/vsys-approval.htm) before a voting system can be used by a jurisdiction. This is a requirement that can be amended by the California Secretary of State via administrative order. The U.S. Election Assistance Commission (EAC) handles federal testing (see www.eac.gov/testing_and_certification/testing_and_certification_program.aspx). Testing is done by labs accredited by the EAC, which are known as voting system test laboratories.

In the federal certification process, any modification to a voting system requires a re-testing of the entire system, even if the change is to an isolated part of the system. Therefore, even a small change to a voting system will require a very significant investment to achieve re-certification under the federal process. Estimates on the cost of federal certification vary, but most estimates are above one million dollars.

Transparency, Source-Code Disclosure, Licensing, and Contingency Planning

Sequoia Voting Systems developed San Francisco's current voting system using the company's own proprietary system design and software development methodologies. The source code has been reviewed by some voting experts and regulators, but the majority of the system is not open-source and is not available for the general public to inspect which makes is difficult for voters to establish confidence that the software is free of unknown software defects or design flaws. It is difficult to replace any aspect of the current voting system because the code is neither open-source, nor designed with clear modules.

The ability to review source code and systems design is an essential property of a trustworthy voting system. By giving the public access to the source code of a voting system, there is an increased chance that a defect will be found in a voting system, whether by a member of the election administrator or a member of the public. Joseph Hall's paper "Transparency and Access to Source Code in Electronic Voting" (http://josephhall.org/papers/jhall_evt06.pdf) includes ideas for contingency plans to address possible discoveries.

Innovation

Although jurisdictions across the United States have expressed interest in using alternative voting systems, most have not been able to go beyond researching and reporting on alternatives. Running a county-wide election is very complex, so it can be risky to try out new technologies. Several jurisdictions have tried out innovative solutions by initially testing redundant systems in limited ways in order to independently verify the accuracy of election results from the jurisdiction's proprietary voting systems.

While we have been discussing innovation for a jurisdiction's official results, there are several innovations for independently confirming the results of a jurisdiction's official system. One example is Takoma Park, MD, which used an open-source system called Scantegrity (www.scantegrity.org/) in a municipal election (e.g. an election with no state or federal races.) Another is Humboldt County, which used the Trachtenberg Election Verification System (TEVS), as part of the effort called the Humboldt Transparency Project (http://humtp.com and www.humett.org). TEVS has been used in every election since November 2008 and is discussed further in the Election Records and Post-Election Audit section of this document.

Software Best Practices

There are standard Software Engineering best practices that have been found to create more reliable, maintainable software. These include making sure code has ample unit-tests and is built using well-defined modules. An open-source license does not ensure that code is high quality, so it is important to make sure that any voting system under consideration has been built using best practices that have been accepted across the software industry.

Recommendations

Business and Partnership Models

The VSTF supports the DOE's stated intention to renew its contract with Sequoia Voting Systems through 2013 with the stipulation that the short-term recommendations contained in this report, particularly concerning auditing, are implemented whenever feasible.

The DOE should use the intervening three year period to consider a broad range of possibilities regarding the business and partnership model it will pursue to acquire/develop San Francisco's next voting system, including collaborating with other jurisdictions, academic institutions, or non-profit organizations. Specifically, the DOE should reach out to Los Angeles County with the goal of monitoring the work of its Voting Systems Assessment Project. The DOE should also consider reaching across the bay to Alameda County, which shares some similar requirements, notably Ranked Choice Voting.

The DOE should take current academic research into account to ensure that this work is considered in the selection of the City's next voting system. The DOE should also closely monitor innovations in the voting systems marketplace to determine if new products that meet the minimum requirements outlined in this report may be available in the required timeframe.

Certification

The VSTF recommends that the City and County of San Francisco advocate with the California Secretary of State that a comprehensive state certification process replace the existing requirement for federal certification. The state should aspire to a certification process that is more agile, efficient, and cost effective to enable innovation.

Transparency, Source Code Disclosure, Licensing, and Contingency Planning

The DOE should be an active participant in the movement toward more open and transparent voting systems. Open systems will enable better security and lessen the chance that there is an unknown software defect or design flaw that affects the integrity of an election. The DOE should give strong preference to a voting system licensing structure that gives the City and County of San Francisco all of the rights provided by an OSI-approved license, even if the system is maintained by an external party.

If an open-source model is used, the VSTF recommends that the City of San Francisco work together with other jurisdictions and organizations to develop and manage the code-base in order to leverage additional resources and expertise. The City of San Francisco should participate during the Requirements Gathering stage of development so that its unique requirements can be incorporated into the system design and implementation.

If circumstances dictate that a solution that provides an OSI-approved license cannot be implemented by the time the contract for the City's current system expires at the end of 2013, the

City and County of San Francisco should purchase voting equipment and services from a vendor who will provide a system with the following minimum characteristics, irrespective of the other details of the license:

- Anyone can review the source code of the entire system
- Anyone can run code for testing
- Anyone can distribute changes to code (i.e. documentation on defect and defect fixes can be distributed openly)

The DOE should set up a contingency plan in case a defect is found in the source code of the voting system. The DOE should set up a volunteer committee of experts that can rapidly address any discovered defects and take appropriate action to address those defects. The committee of experts should include computer scientists with expertise in voting systems and security and members of the DOE with deep knowledge on the voting systems and procedures in San Francisco.

Innovation

It should be the policy of San Francisco to conduct pilot projects of alternative election technologies and procedures. This could initially involve small elections or a small number of precincts. These pilot projects would provide opportunities to learn how well alternative approaches work, such as using open source systems, and hand counting paper ballots at the polling places. All results of a pilot project should be confirmed using hand-counting.

Software Best Practices

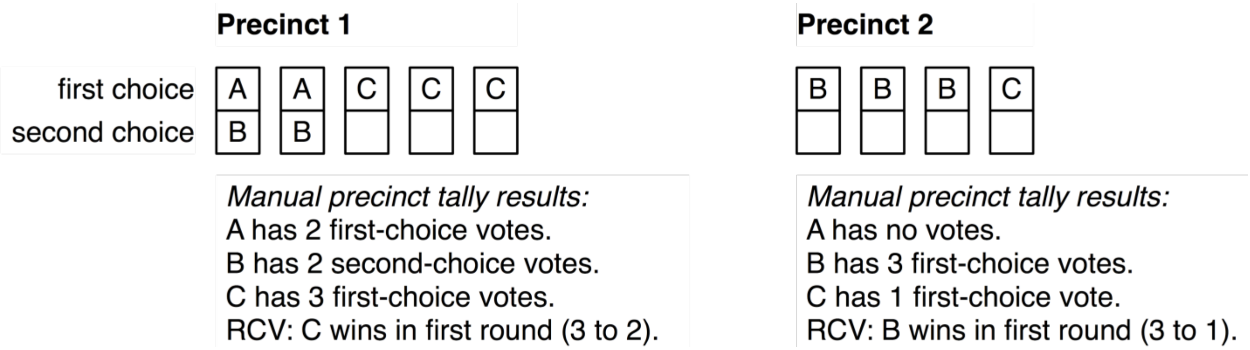
All voting systems software should be designed and implemented using the following modern, high-quality industry methodologies:

- Peer reviews of source code should be done throughout development of the new voting system.
- All source code should include extensive unit tests.
- The system should be modular in design with open data formats for exchanging data.
- There should be well-documented code, a clear technical architecture, and a detailed database design.
- The system should be delivered with extensive administrative (i.e. election workers) and end-user documentation (e.g. how system will be used by voters, including voters with different accessibility requirements.)

Section 3

Appendix A

This appendix shows that the RCV manual tally process currently used in San Francisco does not audit the outcome of an election. Consider the following example of an RCV contest with three candidates (A, B, and C) and two precincts (5 ballots in Precinct 1, and 4 ballots in Precinct 2):

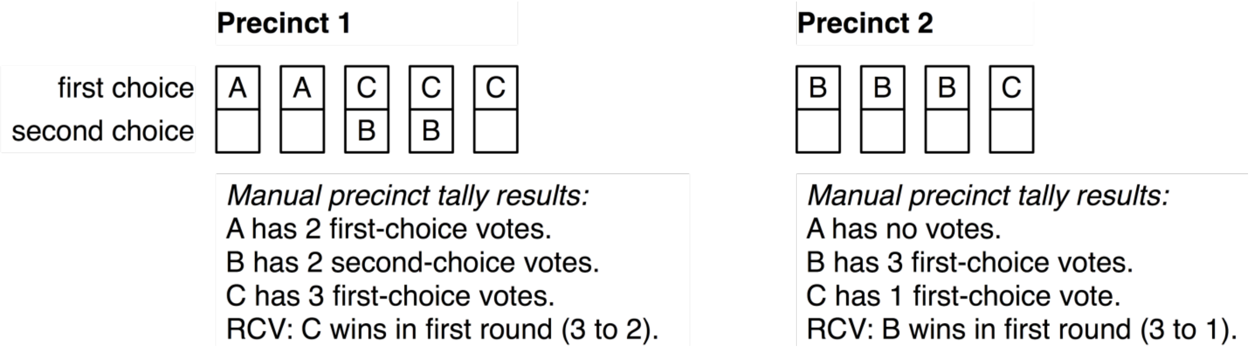


Manual precinct tally results:
A has 2 first-choice votes.
B has 2 second-choice votes.
C has 3 first-choice votes.
RCV: C wins in first round (3 to 2).

Manual precinct tally results:
A has no votes.
B has 3 first-choice votes.
C has 1 first-choice vote.
RCV: B wins in first round (3 to 1).

When all 9 ballots are counted together, no candidate has a majority of first-chobice votes. Candidate A is eliminated, transferring 2 votes to Candidate B. In the second round of counting, Candidate B now has a majority (5 out of 9 votes) and wins the election.

Compare this to an alternate scenario with slightly different votes cast:



Manual precinct tally results:
A has 2 first-choice votes.
B has 2 second-choice votes.
C has 3 first-choice votes.
RCV: C wins in first round (3 to 2).

Manual precinct tally results:
A has no votes.
B has 3 first-choice votes.
C has 1 first-choice vote.
RCV: B wins in first round (3 to 1).

When all 9 ballots are counted together, again no candidate has a majority of first-choice votes, and Candidate A is eliminated. In the second round of counting, Candidate C now has a majority (4 out of 7 votes) and wins the election.

Notice that in both scenarios, manual tallies *within each precinct* produce exactly the same results. The total number of first-choice and second-choice votes for each candidate is the same. The RCV procedure, carried out within each precinct, produces the same result. So, even a 100% manual tally, using the current procedure, cannot distinguish these two scenarios—yet they yield different winners. This demonstrates that the current manual tally procedure does not correctly assure the RCV election outcome.

Appendix B

Ranked-Choice Voting Considerations

Ranked-Choice Voting (RCV) is the law in San Francisco. In March of 2002, San Franciscans passed Proposition A, thereby adopting an amendment to the City Charter making Ranked-Choice Voting the method of electing city and county office holders.

Therefore, the VSTF takes the existence of RCV in the City and County of San Francisco as its baseline and does not make recommendations about retaining or rejecting this method of voting. However, related processes and procedures have been considered, notably in the Elections Records and Post-Election Audit Procedures section.

To summarize, RCV - as opposed to a plurality or other summable method of determining the outcome of an election - does present challenges that have implications for voting systems and related procedures. To determine the RCV result, each ballot must maintain its identity as ballots are counted. Thus, the software and algorithms for tabulating the election results are more complex than in the summable election method. The process of auditing the election is made more complex in that a precinct level audit can only provide confidence on the accuracy of the voting system data as recorded from the paper ballot but not the election result. San Francisco's procedures do provide for a precinct "simulation" of the RCV elimination process, but this type of audit does not provide valuable results to increase confidence that the race was properly tallied.

This report does not examine software complexities of RCV. There is not an inherent problem in programming for RCV logic other than the fact that there is more coding involved which in itself does not impugn the integrity of RCV as a voting method or any voting system used to count it. Transparency is important to produce confidence that a voting system will properly record and tabulate the result of RCV and non-RCV contests. This report does evaluate audit procedures and does make recommendations that will strengthen audits in general and specifically for RCV contests.

Section 4

About the Voting Systems Task Force

The VSTF has seven members with backgrounds in good government, computer science/software development, and accommodations serving persons with disabilities. Members serve as individuals and represent no other organization or group. Members include:

Jody Sanford, Chair
Ka-Ping Yee, Vice-Chair
Roger Donaldson
Tim Mayer
Beth Mazur
Gregory Miller
Jim Soper

The VSTF began work in May 2009 and held public meetings at least monthly. It conducted research and solicited feedback (February 2010 and January/February 2011…now underway) to produce the recommendations contained in its final report. The task force "sunsets" on June 30, 2011.