State Budget Matching Funds Proposal for Counties to Develop an Open-Source Paper Ballot Voting System

CALIFORNIA CLEAN MONEY CAMPAIGN

SUMMARY

The California Clean Money Campaign is proposing an allocation of $8 million in the state budget for the Secretary of State to provide matching funds to one county to help expedite its development and certification of a publicly owned open-source paper ballot voting system. The matching funds would only be eligible to develop a system licensed so that all counties can freely use and build on it to lower costs and increase security and confidence in elections.

Assemblymember David Chiu and Senator Scott Wiener submitted a budget request letter on April 13th matching the outlines of this proposal.

BACKGROUND

The cost of replacing California's voting machines with new proprietary voting systems is astronomical. The current 2018/2019 state budget proposal includes $134.348 million for the Secretary of State for "Voting Replacement for Counties" to replace voting systems in a joint venture between the State and counties, with a 50/50 split. But it's just a start because AB 668 (Gonzalez-Fletcher) contemplated total costs of $600-$675 million to replace counties' voting machines.

Worse, proprietary voting systems lack transparency and have proven vulnerable to security threats. At the 2017 DEF CON security conference testing proprietary voting systems "every piece of equipment … was effectively breached in some manner". Their report concluded it was a ***"national security threat".***[1]

In contrast to the secret, proprietary software created and controlled by private vendors, open-source paper ballot voting systems would be openly licensed and therefore transparent and open to public inspection.

Former CIA director James Woolsey said:

> *"If we are to properly defend against outside (and possibly inside) interference, or "hacking," the software can not remain private and secret. For national security, the election system software must be what is used by NASA, the Air Force, and the Department of Defense. It must be open source."*[2]

The Department of Defense Open Source Software FAQ states why it uses open-source for security:

> *"Making source code available to the public significantly aids defenders and not just attackers. Continuous and broad peer-review, enabled by publicly available source code, improves software reliability and security through the identification and elimination of defects that might otherwise go unrecognized by the core development team. Conversely, where source code is hidden from the public, attackers can attack the software anyway."*[3]

An open-source paper ballot system licensed under the GNU General Public License 3.0 would be freely available to any county to use and modify, with any improvements always remaining public and benefiting all counties. **Experts estimate it would cut the overall cost of new voting systems in half.**[4] This would save the state and counties hundreds of millions of dollars, make elections more secure, and increase confidence in their reliability and transparency.

A February California Clean Money Campaign poll of 772 likely voters found that by a 4-1 margin they supported "having the California state budget provide matching funds to help counties develop and certify publicly-owned, open-source paper ballot voting systems" (66% Yes, 17% No, and 17% Undecided).

As Secretary of State Padilla said, *"Open source is the ultimate in transparency and accountability for all."*

PROPOSED SOLUTION

We propose allocating $8 million in the state budget for the Secretary of State to provide matching funds to one county to develop an open-source paper ballot voting system, with the following constraints:

- The system must be licensed under the GNU General Public License 3.0[5] to ensure that other counties may use and modify it while keeping it permanently open source and available to the public.

[1] "DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure", 9/2017.

[2] "Securing US election systems: Why a paper ballot isn't enough", by R. James Woolsey and Brent Turner, Op-Ed in the San Francisco Examiner, February 14, 2018.

[3] DoD Open Source Software (OSS) FAQ, http://dodcio.defense.gov/Open-Source-Software-FAQ

[4] "Publicly-owned voting systems could reduce costs by 50%", California Association of Voting Officials, 1/2015.

[5] All parts of system paid for by the county or state must be exclusively licensed under GPL 3.0 or higher. Other parts of the system must use OSI-approved open source code.

For more information:
Printed in-house
(Updated 5/8/18)

California Clean Money Campaign
3916 Sepulveda Blvd., Suite 208 ♦ Culver City, CA 90230
Phone (800) 566-3780 ♦ www.CAdisclose.org ♦ info@CAclean.org

State Budget Matching Funds Proposal for Counties to Develop an Open-Source Paper Ballot Voting System

CALIFORNIA CLEAN MONEY CAMPAIGN

- Matching would be available on a 2-1 basis if the system is used in a pilot project by the Nov 2020 election and also certified by the Secretary of State.
- Matching would be available on a 1-1 basis if the system is used by the November 2022 election.
- If a full system isn't complete by deadlines, funding for components that have been demonstrated and certified will be eligible for the matches.
- The county immediately receives matching funds upon its own allocation of funds, but must pay back any extra it received depending on goals achieved and whether it has certified a tabulation system.

Compared to the $134 million in matching funds proposed in the budget to start replacing proprietary voting systems, this relatively modest $8 million budget investment in public open-source systems would save California and its counties tens of millions of dollars after they've been certified because every county will be able to use and build on them for free.

Though we also need strong chains of custody and statistically sound manual post-election audits to secure elections, open-source paper ballot voting systems will increase transparency of vote counting, earn voters' trust, and help California lead the nation to more secure elections.

CONTACT

Trent Lange
President, California Clean Money Campaign
(310) 428-1556, tlange@caclean.org

QUESTIONS AND ANSWERS

What is open source paper ballot voting?
Open source software, in contrast to secret proprietary software, is free for anyone to inspect, use, and improve. That allows "many eyeballs" to examine the public code to find security flaws or other problems. The open-source approach we're backing prints and uses paper ballots that can be audited and hand-counted when needed.

Is open source software more or less secure than proprietary software?
Independent studies have shown that, in general, open source software when written is neither more secure nor less secure than proprietary software (see for example Synopsys's "Coverity® Scan Open Source Report 2014"). Both secure and insecure open source software can be written. Similarly, both secure and insecure proprietary software can be written.

A key difference, though, is that, because it is publicly viewable, claims about the security of open source software can be independently verified by anyone (provided they have the necessary skills and time). With proprietary code, such claims can be based only on trusting those who are able to view the code.

The security of a given piece of software is primarily a function of how well the software is written and tested. It doesn't depend on keeping the code secret. The idea that software can be made secure by keeping it secret is an idea known as "security by obscurity" and is widely rejected in the security community.

Open source is already heavily used and relied upon throughout the world for security-critical applications. For example, much of the code that allows the secure transmission of information over the internet is open source, as is much of the software used by NASA, the Air Force, and the Department of Defense.

How can members of the public be sure that the open source code is running on the machine?
The short answer is that there is no way to be certain that the code running on a particular device or computer is what one expects it to be, whether the software is open source or not. This is an extremely hard problem to solve and is an active area of research. One reason is that there is no way to be sure that the computer hardware itself can be trusted.
Having said that, good auditing practices that involve randomly checking computer results by hand against the original paper ballots are an adequate countermeasure, provided the audits are done correctly. This is why good audit procedures are important when computers are used to count ballots.

Shouldn't we hand-count all ballots?
Full hand-counting of ballots might be a good idea, but would be an expensive and long process in California with over 13 million votes cast. Even if California did full hand counting, we'd still want a quick and reliable open-source count right away to make it less likely that Tammany Hall-style ballot-stuffing could be hidden in the days it may take for a full hand count.