FAQ for AB 1784, the Secure the VOTE Act (Santiago-Chiu-Gonzalez)

What does "VOTE" stand for?

"**V**oter-verified **O**pen-source paper ballot **T**ransparent **E**lections"**.**

What will AB 1784 do?

Provide a total of $16 million in state matching funds for counties to develop, certify, and create a governance model for **publicly owned Open-Source Paper Ballot Voting Systems**. Funds are allocated on a first-come first-served basis to counties that agree to reasonable requirements including using an OSI-approved open source license to ensure that other counties can use and modify it for free. Counties are eligible for a maximum of $8 million each.

Why do we need Open-Source Voting Software?

Current voting systems use privately owned secret software that lacks transparency and has proven vulnerable to security threats. At the 2017 DEF CON security conference testing proprietary systems *"every piece of equipment… was effectively breached in some manner"*. Their report concluded it was a *"national security threat"*.

Publicly owned open-source voting systems will also save tens of millions of dollars in license fees currently paid to corporate vendors. It's estimated that it would cost California counties $600 million to replace current aged systems with new proprietary systems. But after a publicly owned open-source voting system is certified, every county will be able to use and modify the software for free.

Open-Source Voting Endorsers (Of 2018 State Budget Request)

- California Clean Money Campaign (Sponsor)
- California Association of Voting Officials
- California Common Cause
- California Voter Foundation
- Californians for Disability Rights
- Courage Campaign
- DailyKos
- Endangered Habitats League
- FairVote California
- GMO Free California
- Harrington Investments, Inc.
- Open Source Initiative (OSI)
- MOVI, Money Out Voters In
- People Demanding Action
- Progressive Democrats of America
- Voting Rights Task Force

Won't it be dangerous for bad actors to see inside the software ("source code")?

No. Most security threats don't need knowledge of source code. Most home computer operating systems use secret code, but "security by obscurity" doesn't work, which is why almost everybody's computer has been successfully attacked by viruses (some repeatedly). In contrast, most web servers use Linux because it is open-source and thus has benefited from "many eyeballs" inspecting it to find potential security flaws and propose fixes.

Is open-source software more or less secure than proprietary software?

While it's possible to have proprietary software that's relatively secure, it's impossible to independently very whether it actually is. "Trust us, our software is secure" isn't good enough for elections.

Because open-source is publicly viewable, claims about its security can be independently verified by anyone (with the skills and time). With proprietary code, such claims cannot be proven and so you have to completely trust the corporation that wrote it. Like everyone else, programmers make mistakes. Open-source voting systems will allow others to catch errors that open the door to meddling that changes the outcome of an election.

Open-source is already heavily used and relied upon throughout the world for security critical applications. For example, much of the software used by NASA, the Air Force, and the Department of Defense is open-source.

For more information:
Printed in-house
(Updated 4/11/2019)

If the code is open-source, how can you stop people from changing it?

The actual code will be controlled by the counties that develop open-source voting systems and receive certification by the Secretary of State. Although the public will be able to review the code to see how it works, search for security flaws, and suggest changes, no one can actually alter the code except county elections officials who must then have their new version recertified by the Secretary of State.

AB 1784 allows the matching funds to used to help the counties create a governance system to protect their open-source code and to provide for sharing, maintenance, and updates.

Will only two counties benefit from AB 1784?

Every county will benefit from AB 1784! The entire $16 million in matching funds may be received by two counties. But to receive the funds, the open-source voting system they develop must be free for other counties to use and modify. To ensure this, the county must release their code under an OSI-approved open source license.

This means that every county will ultimately be able to take advantage of the investment and hard work of the counties that develop and certify an open-source voting system, saving tens of millions of dollars in license fees compared to current proprietary systems.

How can taxpayers and the state be sure the counties won't waste the money?

A county will have to return all the state matching funds by the end of 2026 if they haven't developed an open-source system for tabulating vote-by-mail ballots, licensed it as required, and received certification by the Secretary of State.

Is open-source all we need for secure elections?

Of course not! We also need strong chain of custody of the software, machines, and other materials, plus voter-verified paper ballots (which AB 1784 requires), and statistically sound manual post-election audits. All these things are necessary to secure our elections. But without the transparency of open-source election software – even if we adopted all the other measures listed here -- voters will never be able to know that their votes are counted accurately and are secure. *"Trust us, our software is safe"* isn't good enough for democracy.

"Open-source is the ultimate in transparency and accountability for all."

— Secretary of State Alex Padilla

For more information:
Printed in-house
(Updated 4/11/2019)

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