LOOK
AHEAD
AMERICA

FAQ: Black Box versus Open Source Voting (Version 1.0)
June 2021

What is Black Box Voting?

"Black Box Voting" (BBV) uses secret, proprietary software and hardware to create, count, and adjudicate ballots. Only the manufacturer knows and has access to the software code as well as the schematic designs of the machines themselves. The public and elected officials cannot access the software code or schematics of the machines, in order to understand how the software works.

Governments that purchase BBV systems sign contracts that prevent them from attempting to 'reverse engineer' the software or open up the hardware.

In addition, the BBV manufacturer has a monopoly on updating, servicing, and repairing that equipment, because nobody else has access to the code or schematics.

What is Open Source Voting?

"Open Source Voting" (OSV) relies on code and hardware schematics that are publicly available for review, so anyone can review how they work and identify potential flaws.

OSV does not get "locked in" with any particular vendor for service or repair, since any programmer or technician can have complete access to information about how the machines work.

Is Black Box or Open Source more secure from hacking?

According to a study by Princeton University, BBV can not only be hacked, but can be hacked without ever being detected.[1] Politico Magazine wrote a story featuring a Princeton scientist that hacked a BBV machine in seven minutes.[2]

Then-Senator Kamala Harris testified at a Senate committee hearing that she personally witnessed the manipulation of BBV machines right before her eyes. This account, as well as criticisms about the security of BBV from Senator Klobuchar and others, is featured in the 2020 documentary *Kill Chain: The Cyber War on America's Elections.*

Nearly every major software-based hack of personal information or take-over of computer systems has involved servers running black box software.

Alternatively, because security experts can identify potential flaws and recommend fixes in Open Source software, they widely regard it as more secure than proprietary, "secret" code.

In an article in Government Technology Magazine, Hilton Collins cites multiple government IT experts who explain why open source software has significantly greater security has than black box software.[3] A DevOps Magazine article published on April 21, 2021 also documents the security advantages of open source over black box.[4]

What are the Advantages of Open Source Over Black Box?

There are four big advantages of OSV over BBV:

1. **Security**: Open source is demonstrably more secure than proprietary software.

2. **Public Confidence**: The public can access the code and schematics of OSV, so they can have more confidence that someone has not hacked the election. While not everyone has the ability to analyze the code or schematics, if needed they can rely on experts they trust to ensure the integrity of the voting equipment and election security.

3. **Costs**: BBV allows the manufacturer to have an exclusive right to maintain, update, and repair their voting equipment. With OSV these services remain open to competition, driving down costs significantly.

4. **Home State Jobs**: Rather than relying on out-of-state or even out-of-country BBV vendors to maintain voting equipment, state and county governments can give service contracts to qualified local firms, thus keeping their taxpayers dollars in-state and creating local jobs.

Is OSV Equipment Available?

Yes, for a few different reasons:

1. Voting.Works an American-based company that manufactures open source voting equipment currently in use across multiple states.

2. Voting equipment is a buyer's market. The requirements of the state and local governments— from the way the ballots are tabulated to accessibility for handicap users — drive the designs of the voting equipment manufacturers. Were the government to require open source voting equipment for all of their purchases, then prospective vendors would build to that requirement in order to get the multi-million dollar contracts.

3. Every BBV company could easily become an OSV company by publishing their existing source code and schematics.

Is there bipartisan support for OSV?

OSV is one of those rare issues that has bi-partisan support. For example, the first federal legislation introduced to require nationwide OSV came from scientist-turned-Democrat Congressman Rush Holt of New Jersey. In addition, left-leaning media outlets and mainstream documentaries like *Hacking Democracy* have made the case for open source voting equipment for decades, while more recent documentaries like *The Real Activist* have raised questions about the 2020 General Election, which has rallied many on the right to support OSV.

Furthermore, opposition to dependence on international corporations for the operation of our elections is something that both the populist left and right can agree on.

How can government policies be changed to support OSV?

Advocates can fight for three policies at the federal, state, and local level to support OSV:

1. Ban the use of BBV systems and require the purchase of OSV machines for use in all future elections.

2. Require state and federal regulatory agencies to certify only OSV machines for use in elections, or at least open the door for OSV machines to be certified. OSV are currently blocked from being approved by the Federal Election Assistance Commission, and many states rely on that certification in selecting voting equipment.

3. Fund grants to support the creation and certification of OSV solutions.

What about paper ballots?

Nearly all current OSV and BBV solutions use paper ballots, as they are an inescapable requirement of mail-in absentee voting. Requiring them as part of the design specification for all future state and local voting equipment purchases remains fully compatible with an OSV requirement, since pure paper ballot solutions involving no machine counting are inherently open source.

About Look Ahead America

Look Ahead America is an America First 501(c)3 nonprofit dedicated to standing up for patriotic Americans who have been forgotten by our government. That means deploying our R.E.T. (Register, Educate, Turnout to Vote) field programs across the country. It means leading Patriot Actions and training citizens to lobby their state and local governments for America First causes. And it means ensuring voter integrity by investigating cases of illegal ballots and advocating for election reform to prevent them from being cast in the first place.

To learn more about LAA or to support the organization, please visit https://www.lookaheadamerica.org.

[1] https://citp.princeton.edu/our-work/voting/
[2] https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144/.
[3] https://www.govtech.com/security/is-open-source-software-more-secure.html
[4] https://devops.com/is-open-source-more-secure-than-closed-source/