

Dear Elections Assistance Commissioners and all interested parties:

We write this letter of concern and solution proposal after speaking with many members of the federal, state, and county governments. Thanks to EAC Director Hancock for encouraging this letter.

It is our assumed duty to again reach out in hope of providing information regarding election system security and best practice. The undersigned is a collective of concerned citizens and technologists focused on protecting our United States election systems from manipulation. Our represented group partially consists of technologists, solution providers and activists.

It is our understanding and conclusion that, as of this date, there has been little progress toward properly securing the election systems for the United States. This is the cause of our grave concern. It is our further conclusion and concern that although properly defensible election system technology is available for deployment, that technology is being deterred and delayed by corporations attempting to protect market share and shareholder interest to the detriment of the national security.

## 1. BACKGROUND

For context, in 2004 Open Voting Consortium demonstrated an open source election system:

<https://www.nytimes.com/2004/04/01/business/technology-briefing-software-voting-software-to-be-demonstrated.html>

In 2005, the Government Accountability Office directed the technology transfer aspect of a National Science Foundation multi-million dollar grant (grantee ACCURATE) to include the open source pioneering work of Open Voting Consortium. This directive was ignored by the ACCURATE group and that grant money yielded no specific public benefit. Other disturbing activity has been noted attached to the ACCURATE absorption of the grant.

In 2006, Dr. Rebecca Mercuri filed documentation of inappropriate action by the ACCURATE working group with the NSF's Inspector General :

<http://www.notablessoftware.com/ACCURATE/ACCURATE.html>

This initial diversion away from open source voting systems caused substantial delay and altered the United States government's path toward proper election system security. To this day, the same controlling group from ACCURATE (i.e., David Dill -VERIFIED VOTING) has tendered opinion at the highest levels of government. Currently the affiliate network under VERIFIED VOTING (Center for American Progress , League of Women Voters, Lawyers Committee for Civil Rights, etc. ) is properly touting audits and paper ballots, but improperly continuing to omit the necessary component of open source technology. This is hereby noted and the opinion assumed affected by corporate interests:

<https://www.nytimes.com/2017/08/03/opinion/open-source-software-hacker-voting.html>

<http://www.sfexaminer.com/securing-u-s-election-systems-paper-ballot-isnt-enough/>

Conversely, there has been election system security progress in the State of New Hampshire with Dr. Juan Gilbert's open source, paper ballot Prime III system. The State of Ohio recently certified open source software for absentees and San Francisco County has allocated 1.7 million dollars toward the initial build-out of an open source election system project:

<http://news.ufl.edu/articles/2016/05/how-universal-design-can-help-every-voter-cast-a-ballot.php>

[https://www.theregister.co.uk/2016/02/10/san\\_francisco\\_to\\_open\\_source\\_voting\\_systems/](https://www.theregister.co.uk/2016/02/10/san_francisco_to_open_source_voting_systems/)

## 2. INTERFERENCE WITH U.S. ELECTIONS

It is now generally acknowledged that the proprietary election systems sold by vendors to the United States via Help America Act funds are deficient and cannot be cured by the mere addition of a paper ballot or an after the fact audit. Though ballots and audits are ostensibly in the positive column, the position of experts is that the software cannot remain private and secret as “security by obscurity” is now recognized as a failed concept. The scientific position for open source software voting system security is further bolstered by the conclusions of NASA and the DOD. Experts omitting this piece of the security conversation must be questioned regarding source of motivation. Also, technologists devising new licenses under the banner of open source are likewise properly scrutinized for motivation. Los Angeles County has recently announced an “open source” system but has not revealed the software. See the Los Angeles County “open source voting” project:

<https://statescoop.com/los-angeles-countys-new-open-source-vote-tallying-system-isnt-open-source-just-yet>

It is fair to state some of the same experts omitting open source solutions to the election system crisis in advocacy work are also pushing for the purchase of yet another round of proprietary voting systems. This is an untenable position in the wake of the intelligence community findings of easily conducted interference with the proprietary systems.

## 3. OUTREACH TO GOVERNMENT FROM THE PRIVATE “DO-GOODER” SECTOR

The National Association of Voting Officials was formed as California Association of Voting Officials with a mission toward education and availability toward a public–private open source voting software quality assurance program. CAVO / NAVO and its preceding OVC has reached out to veritably ALL politicians and good government groups in the election security space for the purpose of heightening awareness and moving toward the deployment of solution voting systems. The response has been less than stellar as the time frame windows now close on our ability to secure the U.S. voting systems by 2020. Political will ebbs and flows as Microsoft and those government advocacy groups who “bob in their wake” continue to cause delay via fear, uncertainty and doubt tactics.

## 4. VENDORS SEEKING TO LOCK IN PRIVATIZATION OF ELECTIONS CONTINUE TOWARD FAILED SECURITY

[https://motherboard.vice.com/en\\_us/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states?utm\\_campaign=sharebutton](https://motherboard.vice.com/en_us/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states?utm_campaign=sharebutton)

<https://www.yahoo.com/news/former-trump-official-no-one-minding-store-white-house-cyberthreats-090017630.html>

## 5. LOS ANGELES COUNTY

As the U. S. largest jurisdiction, many have awaited the unveiling of the new Los Angeles voting system. Though the design is less than optimal as it is based in proprietary hardware (with reference appropriate to the sole source contracts inherent), the promised software is open source. Unfortunately, as of the date of this letter, Los Angeles County has not evidenced their claims that the voting system will actually be open source as defined by Open Source Initiative and other recognized authorities. The EAC should also make public statement that the definition of open source is in keeping with the OSI definition:

<https://opensource.org/osd-annotated>

More specifically, the following language in a proposed California ballot measure for 2020 (Election Transparency and Security Act of 2020) includes the meaning of open source voting. Please see clauses Ch.5, Article 1, 19401 of the measure:

(c) “Open source software” means software actually distributed to the public under software licenses that provide that every licensee is free to make copies of the software or derivative works thereof, to distribute them without payment of royalties or other consideration, and to access and use the complete source code of the software.

(d) “Open source voting system” means a voting system that uses open source software for all voting-specific components.

## 6. CONCLUSIONS AND SOLUTIONS

Based on the above statements the undersigned are agreed that the security interests of the United States of America are best served by the immediate creation, certification and deployment of General Public License open source election systems to replace proprietary voting systems. These open source voting systems should be deployed (with paper ballots and robust audits) as soon as possible. The Elections Assistance Commission should waive (as a national emergency) any and all fees for such systems to apply for and complete immediate certification.

Also, The EAC, NIST, DNI, DHS, and all other relevant bodies should convene in an emergency setting to devise best methods of creating public-private partnerships for the said purpose of the aforementioned open source voting system deployment. The EAC should also, as stated in section 5 herein, make public statement that the definition of open source is in keeping with the OSI definition.

Respectfully submitted,

Brent Turner  
Secretary  
California Association of Voting Officials

