Brent Turner Statement to Hoover Commission 7/26/18

Many know the history of this movement to secure US elections. In 2000, standing on the shoulders of Medgar Evers and other civil rights leaders, Alan Dechert and Open Voting Consortium pioneered open source voting systems. Seven years later we started a campaign to have SF lead the country toward safe and secure elections. Since then we have seen open source systems deployed in New Hampshire. Then the 2016 election happened

In New Hampshire, National Association of Voting Officials has worked with Secretary of State Bill Gardner to lead the country by deploying Dr. Gilbert's open source system. We are currently moving toward the completion of that system. Most recently Ohio has now certified the absentee aspect of the open source system

We have all witnessed the multi-million dollar boondoggle of Los Angeles voting and their historic mismanagement. We have witnessed the proprietary code sellers collapse the Texas voting system project. However, in San Francisco County, CA we have overcome faux expert groups like Verified Voting and OSET , as well as the vendors and the lobbyists to be another shining light for democracy. The science is available and the project is manageable without the fear , uncertainty and doubt peddled by corporate interests. The open source voting language is now being carried by Congresswoman Tulsi Gabbard as endorsed by most top scientists , with additional endorsement being made by The National Federation for The Blind- - FairVote – Former CIA Director R. James Woolsey – and the National Organization of Women among many others

Please be aware the real documented pioneers of the open source voting work are available for your benefit. Although Verified Voting and others may absorb most all grant monies and media coverage, these sleight of hand tactics are also part and parcel to the current lack of progress and general confusion. Verified Voting and Phillip Stark know that open source software is a necessary element for proper security, yet they often omit open source software or backseat reference it as " no panacea " when presenting information on paper ballots and audits. This omission smacks of corporate influence and is obviously intended to

enable / create the purchase cycle of more proprietary voting systems that will be no more secure than the current ones. For the reasons stated we reject their corporate software influences and request attention be directed toward more reliable and less biased information. We have included two articles from former CIA Director Jim Woolsey on point

We hope the Hoover Commission follows up on this information.

Respectfully submitted,

Brent Turner

Secretary

California Association of Voting Officials

The New York Times

OP-ED CONTRIBUTORS

To Protect Voting, Use Open-Source Software

By R. James Woolsey and Brian J. Fox

Aug. 3, 2017

Although Russian hackers are reported to have tried to disrupt the November election with attacks on the voting systems of 39 states, the consensus of the intelligence community is that they were probably unsuccessful in their efforts to delete and alter voter data. But another national election is just 15 months away, and the risk that those working on behalf of President Vladimir Putin of Russia could do real damage — and even manage to mark your ballot for you or altering your vote — remains.

Since the debacle of the 2000 election (remember hanging chads?) American election machinery has been improved to reduce the chances of mis-tallying votes, outright fraud and attacks by hackers. These improvements brought with them a new concern: lack of software security. Most voting machines' software can now be easily hacked. This is in large part because the current voting systems use proprietary software based on Microsoft's operating system.

One post-2000 change — a useful one — was to move away from all-electronic touch-screen balloting, with no paper record indicating how someone voted. Nearly half of voters are registered in jurisdictions that use optical-scan systems that read marked paper ballots and tally the results. But one-quarter of voters still use direct-recording electronic voting machines, which produce no paper trail.

At polling places where voting machines don't provide this backup record, there's no way for election officials to run an effective recount if the electronics are hacked.

That's why the National Association of Voting Officials is leading a movement to encourage election officials to stop the purchase of insecure systems and begin to use software based on open-source systems that can guard our votes against manipulation.

But there's resistance to this obvious solution. Microsoft and companies that bob along in its wake don't want their proprietary voting systems replaced by open-source software balloting systems, have aggressively lobbied against them.

Open-source software is simply software for which the original source code is made freely available and may be redistributed and modified. In the case of voting, open-source software systems would be overseen by public-private partnerships between counties and vendors.

Open-source systems are tried and tested. A majority of supercomputers use them. The Defense Department, NASA and the United States Air Force all use open-source systems, because they know this provides far more security. Every step in our voting process should use software that follows these examples.

Despite its name, open-source software is less vulnerable to hacking than the secret, black box systems like those being used in polling places now. That's because anyone can see how open-source systems operate. Bugs can be spotted and remedied, deterring those who would attempt attacks. This makes them much more secure than closed-source models like Microsoft's, which only Microsoft employees can get into to fix.

One reason for the software companies' resistance is the belief that it's impossible to make a profit from open-source software. This is a myth. Businesses that use open-source software still need all of the other things that software companies provide. Many major companies use open-source software in their products.

Open-source systems are already playing a role in some elections. New Hampshire has used them to allow disabled voters to fill out ballots online or on their phones, while Travis County in Texas, San Francisco and Los Angeles have allocated funds to move toward open-source voting systems.

If the community of proprietary vendors, including Microsoft, would support the use of open-source model for elections, we could expedite progress toward secure voting systems.

With an election on the horizon, it's urgent that we ensure that those who seek to make our voting systems more secure have easy access to them, and that Mr. Putin does not.

R. James Woolsey is a former director of the Central Intelligence Agency. Brian J. Fox, the creator of the Bash open-source software, is the lead technologist of the National Association of Voting Officials and the California Association of Voting Officials, which develop open-source voting systems for use in public elections.

A version of this article appears in print on Aug. 2, 2017, on Page A19 of the New York edition with the headline: To Protect Voting, Use Open-Source

NEW HAMPSHIRE
DEPARTMENT OF STATE

William M. Gardner
Secretary of State

Robert P. Ambrose
Senior Deputy Secretary of State

David M. Scanlan
Deputy Secretary of State

Anthony B. S. Stevens
Assistant Secretary of State

May 13, 2016

To: Brent Turner (California Association of Voting Officials)

Re: **one4all**, New Hampshire's Open Source Accessible Voting System

Following the passage of the Help America Vote Act of 2002 ("HAVA"), the New Hampshire Department of State initiated a planning process to satisfy HAVA Section 301, requiring an accessible voting system , by involving election officials and a range of persons with disabilities. When we found that potential users of such a system could not agree on a preferred system, we decided to proceed with a cost-effective and workable solution, with an explicit plan to replace it when we found a system more satisfactory to all.

In 2014, we found a version of open source software that Dr. Juan Gilbert and his Prime III team had made available to the public. With the active support of Dr. Gilbert's Prime III team and the good work of the California Association of Voting Officials, we used it in several pilots in New Hampshire polling places in both the 2014 State Primary and General Election. People with disabilities and election officials responded very positively.

With that experience behind us, we decided to implement the system statewide in the 2016 Presidential Primary and henceforth. We conducted more user testing, obtained valuable input from the disabilities community and election officials, and designed architecture relying on our internal staff. We used the assistance of the Prime III team to make certain software changes. As time went on, we relied more heavily on our own staff and New Hampshire people with disabilities to revise and improve the user interface, ultimately naming the New Hampshire system **one4all**, reflecting our interest in making this available to a wide variety of individuals – one that is not limited solely to the disabilities community. We believe this goal is in the interest of all participants, because having more users ensures more voter privacy.

State House Room 204, 107 N. Main St., Concord, NH 03301
Phone: 603-271-8238 Fax: 603-271-8242
TDD Access: Relay NH 1-800-735-2964
www.sos.nh.gov email: NHVotes@sos.nh.gov

We purchased commercial off-the-shelf Dell tablets, Brother Printers and other equipment, programmed the Dell tablets with our ballots, distributed the equipment to all of our towns and cities, and trained election officials to use the equipment.

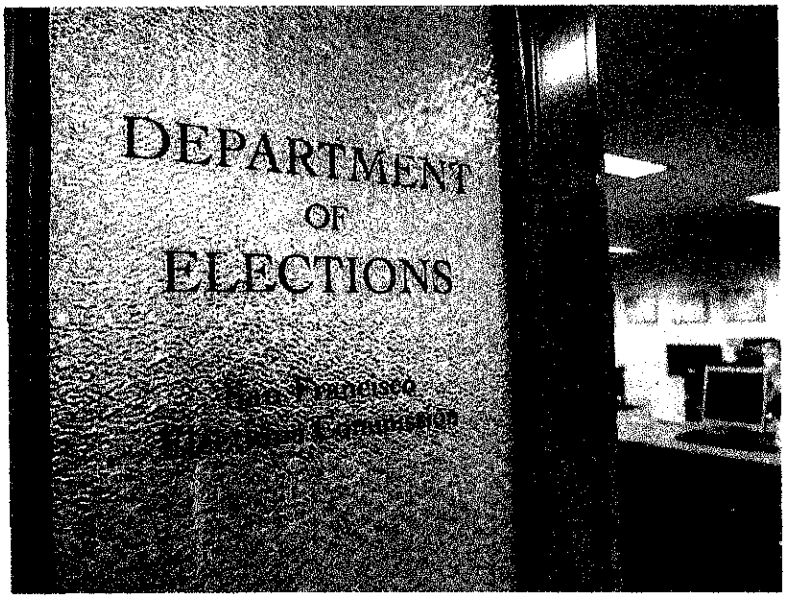
Relying substantially on our internal staff, we are continuing to solve challenges with this system. The beauty of the system is the flexibility of open source and the capacity we develop over time to change the system to reflect user needs. And, of course, it is a small fraction of the cost of the vendor-supplied systems in the marketplace. We look forward to further developing this product in the coming years.

Sincerely yours,
William M. Gardner

State House Room 204, 107 N. Main St., Concord, NH 03301
Phone: 603-271-8238 Fax: 603-271-8242
TDD Access: Relay NH 1-800-735-2964
www.sos.nh.gov email: NHVotes@sos.nh.gov

Examiner
Thursday July 26, 2018

Securing US election systems: Why a paper ballot isn't enough



The Department of Elections inside City Hall in San Francisco is seen Jan. 31. (Mira Laing/Special to S.F. Examiner)

By R. James Woolsey and Brent Turner on February 14, 2018 1:00 am

At first glance, a citizen or "expert" might be persuaded that the way to provide adequate security surrounding the current U.S. election systems is to make sure the systems utilize paper ballots. This is certainly a good idea, but only one piece of the necessary security conversation.

The fact is these systems run on software and the "bugging" of the software is a major vulnerability, regardless of the paper ballot component. 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

Top election system solution technologists language in the Secure Elections Act, a bill introduced by Sen. James Lankford, R-OK, and co-sponsored by Sen. Kamala Harris, D-Calif., is deficient in its failure to address the software code issues. Merely calling for a paper ballot will not provide adequate security.

Trending Articles

Supervisors move to ban workplace cafeterias

Workplace cafeteria ban met with mixed opinions

Muni to improve transit for communities of color, low-income riders

City Hall roasted by D6 candidates promising change for Tenderloin, SoMa

Bonta Hill: San Francisco Giants are stuck as trade deadline looms

software, the systems purchased via the bill will suffer grave threat security vulnerability, allowing outside forces to manipulate our U.S. elections.

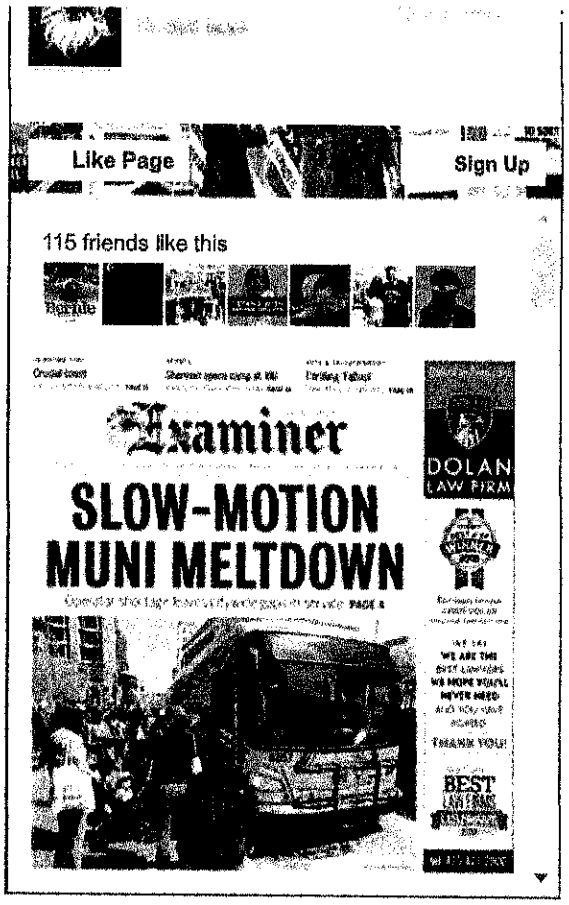
NASA and the DOD, as well as the grand majority of the world's super computers, utilize public software. Regardless of "cybersecurity," the foundation of a proper system is the recognition that "security by obscurity" is generally regarded as a failed concept. It is a far better security environment to have many eyes on the code proofreading for bugs.

Hopefully, legislators will get the message that we now have a historic decision to make regarding our national security. If we are to have secure elections that inspire voter confidence, we should put language in the bill calling for optimal "public" software.

Though some software business interests (and those who "bob in their wake") may not appreciate it, we must do what is best for the national security.

Paper ballots and audits should be included in the bill. But without addressing the software, the bill fails the initial security hurdle. The time is now to get this right. The County of San Francisco is currently taking steps toward an open-source election system that should be the security model for the state and country.

R. James Woolsey is a former director of the Central Intelligence Agency. Brent Turner is secretary of the National Association of Voting Officials and the California Association of Voting Officials, which provide education regarding open-source voting systems for use in public elections.



Click here or scroll down to comment

10 Comments **SF Examiner** **Termie**

Recommend 2 **Share** **Sort by Best**

Join the discussion...

Peter Garland • 5 months ago
Sounds good.
3 ^ v • Reply • Share ›

dwss5 • 5 months ago
Article quote:
—
Our new election systems must have open-source software as well as a paper ballot. If the bill does not call for public, open-source software, the systems purchased via the bill will suffer grave threat security vulnerability, allowing outside forces to manipulate our U.S. elections.
—