Nineteen Election Reform Groups
Oppose Full Public Disclosure of Software on Voting Systems
Want COTS Exemption

April 09, 2007 - updated April 15, 2007

Kathy Dopp

Most independent computer scientists recommend public disclosure of software on voting systems.[i] Current proposals in the US Congress call for full disclosure of voting system software. Here is the wording in Congressman Rush Holt's House Resolution 811 which has 200 House co-sponsors:

> *(9) PROHIBITION OF USE OF UNDISCLOSED SOFTWARE IN VOTING SYSTEMS- No voting system used in an election for Federal office shall at any time contain or use any software not certified by the State for use in the election or any software undisclosed to the State in the certification process. The appropriate election official shall disclose, in electronic form, the source code, object code, and executable representation of the voting system software and firmware to the Commission, including ballot programming files, and the Commission shall make that source code, object code, executable representation, and ballot programming files available for inspection promptly upon request to any person.*

On the other hand, nineteen election integrity groups are demanding an amendment to current federal legislation (HR811) that would exempt commercial off-the-shelf (COTS) software from public disclosure. **Are these election integrity groups advocating for voters or for vendors?**[ii]

FACT 1: "Definition: A component of a computer voting system is considered COTS (Commercial-Off-The-Shelf) if it is (1) general purpose (e.g., operating system software, hardware driver, or database system), (2) not modified, configured, or customized in any manner for voting use, (3) available for sale to the general public" [iii]

FACT 2: COTS software could be trade secret, fully publicly disclosed, or open source (free publicly disclosed software).

(Ed: For simplicity, we ignore the variety in types of licensing agreements for publicly disclosed software. OpenVotingCosortium.org has publicly disclosed voting software.)

FACT 3: There is insufficient legal means to require public disclosure of all trade secret COTS software on voting systems.

FACT 4: There is no technical means to ensure that undisclosed trade secret COTS software does not contain malicious or buggy programs that could deny voting rights or manipulate vote counts. Since COTS software specifications are written by external sources, future changes to the product will not be within control.

FACT 5: Today, there is no *practical* method, even when the software is publicly disclosed, given current voting system design and development methods and the variety of components within one model, to ensure that a particular voting system software actually ran on a voting machine during an election.[iv]

(Ed: Some method of public oversight must be developed, for the government serves at the people's expense and are our employees, and not vice versa.)

FACT 6: There is no infrastructure (equipment, systems, and technologists) available to verify that any voting system software actually ran on a voting machine during an election.

(*Ed: An effective infrastructure could possibly be developed over time if secure voting machines were developed with public disclosure and accountability in mind*.)

FACT 7: Virtually any voting system software could be manipulated to rig elections or to disrupt service to voters. Trade secret COTS software is manufactured in China, Canada, India, and many other countries from which hacking attacks against US military and government computers have already occurred. Trusting trade secret COTS software is trusting tens of thousands of employees in thousands of companies all over America and the world.[v]

FACT 8: Most software on current electronic voting systems (DREs, optical scanners, ballot marking devices, and central tabulating devices) is trade secret COTS software, along with custom software which is integrated from possibly many different COTS components.

FACT 9: Voting systems with substantially less trade secret COTS software could be developed and would be more verifiable and allow for better post-election forensics.

(*Ed: This would just take time - probably over several election cycles.*)

FACT 10: Government could provide incentives to develop open source voting systems, and could stop purchasing voting systems with unnecessary trade secret COTS software on it.

(Ed: The Open Voting Consortium is developing one.)

Yet some election integrity groups and their followers are demanding changes to proposed federal legislation in order to continue the use of taxpayer dollars on trade secret COTS voting system software.

These election integrity groups signed formal requests to amend Congressman Rush Holt's House Resolution 811 to exempt COTS voting system software from public disclosure:[vi]

Alliance for Democracy
Alliance for Democracy - Portland Chapter
Audit AZ
Black Box Voting
Broward Election Reform Coalition
Coalition for Voting Integrity (PA)
Democracy for New Hampshire
Las Vegas (NM) Peace & Justice Center
Main Street Moms (theMMOB.org)
MidHudson Verified Voting
Missourians for Honest Elections
New Yorkers for Verified Voting (NYVV)
North Jersey Impeach Group

Progressive Democrats of America (PDA)
Reach Out America, Nassau Co. NY
Velvet Revolution.us
Voter Action
VotersUnite.org
Voting Integrity Alliance of Tampa Bay (VIA Tampa Bay)

The position of these election reform groups is:

> "There must be no undisclosed voting system software. However, **HR811's proposed HAVA Section 301(a)(9), as currently written, fails to exempt software that is truly Commercial Off the Shelf (COTS)** from public disclosure. The bill must be amended to require true COTS software, such as the Windows operating system and standard printer drivers, to be escrowed and available to officials under confidentiality, but not publicly disclosed."[vii]

Nancy Tobi of Democracy for New Hampshire states:

> "**The prohibition of undisclosed software does not provide any exemption for COTS software** (commercial off the shelf). No existing voting equipment meets this requirement because they all use COTS, and many use Microsoft software. Microsoft will never share its code, and this requirement would make every piece of voting equipment in use today illegal, requiring jurisdictions to replace equipment at a high cost, unfunded by HR 811."[viii]

Note: Neither of the above position statements recommends prohibiting or minimizing the use of federal dollars on trade secret COTS software that is on voting systems. Nor do they recommend increasing the time frames to develop publicly disclosed and open source voting systems. Black Box Voting, Voters Unite, Democracy for New Hampshire, Verified Voting of New York, Voter Action, Alliance for Democracy and others, recommend exempting COTS software from full disclosure or requiring possibly legally unenforceable requirements for partial COTS software disclosure.[ix]

In 2002 Common Cause and PFAW ignored the advice of technologists when they pushed for implementation of in-auditable electronic-ballot voting machines. Today, some election integrity groups are ignoring technologists in proposing a blanket exemption for trade secret COTS software which could make voting systems more costly, less secure and reliable, and certainly less transparent and verifiable.

Nancy Tobi, of Democracy for New Hampshire also, surprisingly, objects to current federal legislative proposals which mandate manual counts of paper ballots in the 2008 election. In her words:

> "**10. Section 328.** Effective Date for Audits. Impossible effective date [2008] for implementation among states for whom no such audit function currently exists."

Why are some election integrity groups saying that voting systems should be comprised of trade secret COTS software when much of the trade secret COTS software on voting systems is unnecessary and makes voting systems less transparent, and often less secure and more expensive than necessary?[x]

Conclusion and Recommendations

Paperless in-auditable digital electronic recording (DRE) voting machines should be replaced immediately with currently available optical scan paper ballot systems before the 2008 election. The 2008 election should be manually audited in sufficient amounts to ensure accurate election outcomes.[xi] After that, federal funds should *not* be spent on voting systems which use trade secret software[xii]; and all voting systems, including DREs, optical scanners, and central election management systems should be replaced within reasonable time frames with fully independently auditable, fully publicly disclosed voting systems with exceptions made only under the most restricted stringent conditions as set by independent computer experts. Expert technologists need to plan reasonable time frames to require reductions in the amount of trade secret COTS software on voting systems and ways to encourage the use of open source voting systems.

At most, the only trade secret COTS software which should be permitted on any voting systems[xiii] purchased with federal funds after 2008[xiv] shall:

- allow for reverse engineering for voting system evaluation and testing as well as publication of evaluation and tests, including but not limited to usability, performance, errors and bugs; and
- be firmware used to run hardware[xv]; and
- disclose any information which is necessary to meet the above requirements.

All other software on voting systems, including all operating system software; and all software for the purpose of casting, counting, reporting, or tallying votes or vote counts; and all customized software on voting systems must be fully publicly disclosed. Plus only fully publicly disclosed compilers or program-handling code shall be used to convert source code into machine executable instructions for all software using on voting systems.

Computer scientists such as Vincent J. Lipsio, Beth Feehan, Charles E. Corry, Doug Jones, and Stanley A. Klein who are experts in voting system software, *not* voting machine vendors or election integrity activists, should determine under what conditions and under what testing requirements, trade secret COTS software should be permitted on voting systems. The recommendations regarding COTS software which were agreed to by consensus of the most recent IEEE P1583 standards group, including those not written into the draft standard[xvi], should be adopted.

Acknowledgements

I received significant help understanding the issue of voting system software from dozens of technologists and computer scientists since 2003. For this particular paper, I received comments and assistance from computer scientist Rebecca Mercuri and from computer scientist Arthur Keller of the Open Voting Consortium, as well as from Dan Lyons and Mark Rothstein.

Endorsements[xvii]

Patricia Axelrod, Litigant in Axelrod v Sequoia, NV; Director of The Desert Storm Think Tank and Veterans' Advocate; Director of The Citizen Advocate

Daniel Joseph Lyons[xviii], Software Developer, System Administrator, and Civil Rights Activist

Lucius Chiaraviglio[xix], Scientific Research Assistant with System Administration, Programming, Software Testing, Electronic and Mechanical Design and Testing, and Engineering Experience

[i] Computer scientists consulting with Congress recommended that voting system software be publicly disclosed and this recommendation was written into the Holt, Tubbs-Jones, Clinton, and Nelson bills. Also independent computer scientists who have worked with the IEEE P1583 standards committee who were not also working with voting system vendors do not want COTS software to be exempt from disclosure or testing requirements. Other resources that describe the opinions of computer scientists on this issue and the complexities of verifying software running on voting systems include:
November 2006 "COTS and Other Electronic Voting Backdoors" by Rebecca Mercuri, Vincent J. Lipsio, and Beth Feehan
http://www.csl.sri.com/users/neumann/insiderisks06.html#197 also posted here:
http://electionarchive.net/docs_other/PositionStatements/COTScacm.pdf
"Comment on the IEEE P1583 Standard" by Charles E. Corry, Ph.D. December, 2004
http://www.vote.nist.gov/ecposstatements/Corry-EAC_comments.pdf
"Comment on the IEEE P1583 Draft Standard" by Stanley A. Klein December, 2004
http://www.vote.nist.gov/ecposstatements/comment-memo-5_3_2.pdf
"Comment on the IEEE P1583 Draft Standard – Part 1" by Vincent J. Lipsio December, 2004
http://www.vote.nist.gov/ecposstatements/2004_1221_COTS_STG_EAC.pdf
"Comment on the IEEE P1583 Draft Standard" by Rebecca Mercuri December, 2004
http://www.vote.nist.gov/ecposstatements/MercuriEACmemo.pdf
and
http://en.wikipedia.org/wiki/Custom_software
http://en.wikipedia.org/wiki/Commercial_off-the-shelf
http://en.wikipedia.org/wiki/Open_source_software
"Avoid Another HAVA Train Wreck: Software Disclosure Requirements are a Good Long Term Goal but Need to Be Redrafted in Current Federal Election Integrity Legislation." By Kathy Dopp and dozens of technologists and computer scientists
http://electionarchive.net/docs_other/dopp/VotingSystemSoftwareDisclosure.pdf
David Wagner, computer scientist in his testimony before the House Admin committee
http://electionarchive.net/docs_other/HearingTestimony/wagner.pdf
Holt's HR 811, A Deceptive Boondoggle -- 10 Blunders to Fix by Bruce O'Dell
http://www.opednews.com/articles/opedne_bruce_o__070221_holt_s_hr_811_a_dece.htm

[ii] This story was removed from OpEdNews.com and I was banned from posting on OpEdNews.com, a progressive web site, after Bev Harris of Black Box Voting called the article "false" ignoring my requests to identify any false statement in the article. I have been receiving emails commending the article from technologists, but have also received emails from Nancy Tobi of Democracy for New Hampshire who says my purpose is to "viciously attack others in the movement and to spread disinformation, lies, and paranoid accusations of plagiarism" Here is a saved copy of the disputed article, along with Bev Harris' request to have it removed:
http://electionarchive.net/docs_other/PositionStatements/BevTries2ShutDownOpEdArticle.htm

[iii] This COTS definition is from the Open Voting Consortium's "Proposed OVC Listed Policies: Second Draft"
http://gnosis.python-hosting.com/voting-project/January.2007/0044.html

[iv] Rivest, or others, could probably devise a method to ensure the code components running on a system. (Could be impractical). They would need to hash the code, and encrypt the hash result.

[v] According to Dr. Charles Corry, Colorado Springs, CO, former IEEE (the Institute of Electrical and Electronics Engineers) member of the voting system guidelines committee for 4 years (& former Marine corporal) October, 2006: "Many of the hard drives and apparently all of the motherboards of the voting machines are Made in China. China is known to be attacking the Dept of Defense, Commerce Dept and other government computers. The motherboard controls the computer and hiding a malicious program in the boot sector of a hard drive isn't much of a trick, one has to assume that some or all of the Diebold voting machines are potentially, even probably controlled by China (Security 101)." And "Diebold is based on Microsoft Windows. No other operating system in the world is as subject to so many viruses, Trojan horses, hack tools, worms, or other attacks."

[vi] Their formal letters objecting to fully publicly disclosed software as proposed by Representatives Holt and Tubb-Jones, and Senators Clinton and Nelson:
"Thirteen Issues with the Holt Bill (HR 811)" by Nancy Tobi of Democracy for New Hampshire also takes current election reform bills to task for requiring independent manual counts of ballots in the upcoming 2008, claiming that any requirement for manual audits should be postponed until 2010. http://www.electiondefensealliance.org/13_problems_Holt811_Tobi
"Essential Revisions to HR 811" by John Gideon of Voters Unite is signed by Black Box Voting, by Verified Voting of New York, by Voter Action and many other major election integrity groups.
http://www.votersunite.org/info/HR811EssentialRevisions.htm
I preserved the April 7, 2007 versions of Voters Unite and Democracy for New Hampshire public position statements here:
http://electionarchive.net/docs_other/PositionStatements/13_problems_Holt811_Tobi.htm
and

http://electionarchive.net/docs_other/PositionStatements/HR811EssentialRevisions.htm

[vii] On April 9, 2007 Bev Harris of Black Box Voting pointed out that in a February 13, 2007 post to a discussion forum, she wrote what she characterizes as a "dissenting opinion" that:

"a) The COTS provision, which allows Commercial Off the Shelf components, is still not entirely satisfactory. These COTS components can be used to destroy election integrity, and many obstacles remain to [a] getting the COTS source code on ALL components into escrow in the first place -- actually, this document says "software", not "source code", which is a potential concern; and [b] making sure it is actually the version used in the election, which is an exceptionally challenging task and current remedies lack both the requirement and the means to do this."

Note that in her post, Harris correctly points out a few of the obstacles of getting the code into escrow and verifying it, but she does not dissent from the basic recommendations; and further seems to want to change "software" to "source code" when in truth, much more than source code is needed to have any hope for verifying software which runs on voting systems.

[viii] Ibid endnote v.

[ix] John Gideon's letter is dated February 13, 2007.

[x] Here is a March 12, 2007 article on the topic of voting system software disclosure written with the help of numerous technologists, "Avoid Another HAVA Train Wreck: Software Disclosure Requirements are a Good Long Term Goal but Need to Be Redrafted in Current Federal Election Integrity Legislation."
http://electionarchive.net/docs_other/dopp/VotingSystemSoftwareDisclosure.pdf

[xi] See "Kathy Dopp's Election Audit Papers"
http://electionarchive.org/ucvAnalysis/US/paper-audits/KathyDoppAuditMathBibliography.pdf

[xii] There should be no blanket exemption for all COTS software. Voting systems should contain the most minimal amount of COTS software that is necessary given available products and resources.

[xiii] Where voting systems are defined as machines or software whose purpose is to create ballot definition files, help voters cast voted ballots, or whose purpose is to tally or report votes or vote counts, including central election management systems. There is no intent to prohibit federal funding from being spent on:

- Publicly disclosed or open source COTS software, or
- proprietary trade secret COTS spreadsheet tools and PCs that could be used to tabulate vote counts on condition that election officials publish all tables of data in those spreadsheets to delimited text cvs files on public web sites as soon as they are finished and before the manual audits and prior to when vote counts are made official, or
- normal trade secret COTS printers used to print out reports that are created on central election management systems.

[xiv] After all paperless DRE voting machines are replaced with currently available paper ballot optical scan voting systems. See http://electionarchive.org/ucvInfo/US/EI-FedLegProposal-v2.pdf

[xv] Trade secret COTS components for I/O devices like disks, CD reader, DVD readers and writers, etc. See also "Proprietary Subsystems in the Diebold TSx Voting Machine – A Chart by Black Box Voting © 2007"
http://www.bbvforums.org/forums/messages/46591/ProprietaryTSx-sm-46690.pdf

[xvi] Representatives of voting vendor companies were on the IEEE P1583 group and neglected to include some positions that were agreed to by consensus of the group which did not favor vendor interests.

[xvii] Anyone who would like to endorse this statement, please contact kathy.dopp@gmail.com

[xviii] According to Dan Lyon ""OpenSource voting software is the public's audit of the voting system. We need that audit." Lyon's resume http://uscountvotes.net/docs_other/PositionStatements/resumes/DanLyons.doc

[xix] According to Lucius Chiaraviglio "Any trade secret software, including the BIOS and other firmware, is a security risk, because it may contain malicious software which may be used to alter, disqualify, or otherwise lose votes, or create spurious votes. Source code escrow is of no help, not only because it will never be subjected to inspection by those who truly need to inspect it, the general citizenry, but because it will be impossible to ensure that the source code in escrow is actually what is on the machines. A more general problem of programmable devices is that it is impossible to ensure that software inspected and approved for use on the devices -- even if fully open source -- is what is actually on the machines when they are used in an election." Chiaraviglio resume
http://uscountvotes.net/docs_other/PositionStatements/resumes/ResumeLuciusChiaraviglio.doc