

**Testimony before the  
Committee on House Administration  
Election Subcommittee Hearing on Election Reform  
March 15, 2007**

**Hugh J. Gallagher, Managing Director  
Election Systems Acquisition & Management Services (ESAMS)**

**Introduction**

Thank you for the opportunity to present testimony regarding the subject of open source software in electronic voting systems to the Committee. I have worked in the election industry for over ten years. I first entered this industry as Chief Operating Officer for a start-up company that was created to develop the next generation of direct record electronic (DRE) voting systems: In point of fact I was employee number 1. The product we developed was the first ever DRE to achieve dual NASED certification for software and hardware/firmware. For the last several years' I have been a subject matter resource to state and local governments on a variety of related election administration and technology issues. These experiences have given me a unique insight to the industry, its participants and technology.

**Testimony**

To begin, I believe that regardless of individual positions on the subject of open source software and by extension verifiable voter paper audit trails, a common goal exists: To make sure that when the American public goes to sleep on election night, they believe that the results of the election fairly represent the will of the people. From this mutual goal I believe all interested parties can find common and reasonable ground on how exactly to make this a continuing reality.

Regarding my position on the topic of open source software for electronic voting systems, I am appreciative of what proponents wish to accomplish. I recognize and acknowledge that a less than favorable perception exists regarding the voting system industry. However, in regards to open source code I can not at this time agree that such an approach would make our elections any more secure and reliable. I personally and professionally believe that requiring vendors to make their software open to public inspection would cause more harm than good. I believe this for the following reasons:

First, and potentially the most obvious is that by opening vendor software to public inspection invites precisely the kind of threat that many individuals believe is caused by the vendor software remaining proprietary: Unscrupulous individuals attempting to influence the election process. These individuals would be presented with a road map which could be used to circumvent system security, and as a direct result system reliability and accuracy. No where has empirical evidence been presented, or litigation substantiated, that vendor personnel have attempted to influence the election process by introducing malicious code. However, if the world of possible individuals having access to the voting system software now were open to the general public, what safe guards could be put in place to prevent malcontents from attempting to influence an election?

Arguments put forth by open source code proponents regarding electronic and physical safe guards built into election processes by election administrators have continuously

been dismissed. Therefore it would seem reasonable that if proponents state that an individual intent on causing mischief because of open source software must have access to the system, and they claim this is not possible due to these same electronic and physical safe guards which they had previously dismissed, then their entire argument to date as been moot – you can not have it both ways. I am not aware of any safety mechanism put forth by advocates to secure the integrity of the software, and by extension elections.

Continuing, under the “Attractive Nuisance Doctrine” of the law of torts, landowners can be held liable for injuries to children caused by a hazardous object, such as a simple swing-set or swimming pool that is likely to attract children, who are unable to appreciate the risk posed by the object. Is it difficult to envision an individual with more talent than common sense, being “attracted” to the open source code of an electronic voting system in order to see what they can do with it?

Recent literature and media accounts are replete with talented, mostly young individuals who took advantage of an inadvertent situation that was presented to them and subsequently found themselves involved in the game of “what can I get away with or do now that I have this information?” We have seen access to banking systems compromised as well as other interests, not to mention our own Department of Defense. Were these attacks and the mischief which resulted intentional or were they happenstance because an “attractive nuisance” presented itself? While I truly believe the proponents are honorable in their desire to ensure the public that through open

source software vendors are not manipulating the election process, can these same proponents make sure that rogue elements of the general public do not do what the vendors themselves have not done?

Are these proponents willing to personally assume the liability associated with a compromised election due to the attractive nuisance of open source software? The vendor community is at least finite in size and appropriate personnel screening and security techniques can be effectively implemented. Can we ensure similar screening and security techniques are applied to the general public? Would we as a public be willing to have our respective banks make public their financial and operations software? How would we react to our insurance companies doing so? Is the risk greater than the reward? I suggest it is.

Secondly, another obvious risk in open source software for voting systems is the loss of intellectual property and the competitive advantages it brings to its respective owner. The preponderance of voting system vendors are privately owned companies. These companies have historically been funded through private equity investment or venture capitalist – financing for new entrants with innovative technologies into the voting system market will follow this historic pattern. Venture capitalist and private equity funds traditionally want to maximize returns and minimize risks. One of the most important risks issues evaluated by such groups looking to invest is the security of intellectual property. In the voting system market place, vendor software represents the most significant part of their intellectual property.

The vendor's intellectual property represents for funding purposes a tangible asset; tremendous amounts of time and money go into protecting these assets as well as ensuring no infringements or compromise impact their potential value. If voting system vendor intellectual property rights on which they base so much of their value become public domain, where is the continued value-proposition for potential investors? What makes the voting system vendor an attractive investment opportunity at this point? How does the voting system vendor sustain its viability?

Hardware aspects of voting system vendors represents incremental advantage – most voting system vendors are not vertically integrated (i.e., own their manufacturing capabilities); fixed and variable costs of hardware do not allow in a competitive market high margins based on hardware alone. Without the protected intellectual property of software which gives the hardware the ability to perform, vendors have no competitive or distinct advantage in which to attract financing. Intellectual property has historically provided the basis for investors to place their resources at risk. Intellectual property is an integral part of value creation in any technology-based company and as such is a critical element in obtaining venture capital. If it is determined that voting system software is not entitled to be protected under the precepts of intellectual property rights, why not decide that the Federal Reserves software for managing money supply and interest rates be open to public inspection? It was developed by a third-party company; its' function is critical to ensuring stability in our country. What would the implications be if the Federal Reserves most intimate software systems were open to public inspection? Would such proponents be so cavalier with our money supply?

And finally, what is the express purpose of open source code for voting systems?

Traditionally, advocates of open source code in the software industry cite several advantages to their position: 1) core software is free; 2) availability of the source code and the right to modify it; 3) the right to redistribute modifications and improvements to the code; and 4) the right to use the software in any way. How do these principals apply to voting system software? I suggest they do not. As stated before, I am not aware of any proposed safe guards or control mechanisms for protecting software in the public domain which has as critical a mission role as voting systems.

## **Conclusion**

A report to the California Legislature on Open Source Software in Voting Systems dated January 2006 conducted by Secretary of State Bruce McPherson specially states impart “Open source advocates point to impressive accomplishments for software developed and maintained according to their principals, with apparent benefits to costs, efficiency, quality and security; however, upon close examination, the open source experience is more limited in scope and specific in application.” None of the principals espoused by open source code proponents are even applicable to this situation. So the question remains: To what purpose does providing public access to vendor software benefit the public? Is the public in general proficient enough to understand the nuances of software development and subsequent coding to achieve requirements identified in voting system standards? No. How would the public know if there was “malicious code”

imbedded in the software? They wouldn't. Who specifically will be responsible for reviewing public code? I am not aware of any plan or organization or rules or bylaws or even secret-hand shakes as to how this would actually work. My inclination is to believe that it will be a "free-for-all." It stands to reason that under the proposed legislation requiring open source code for voting systems we will have a smorgasbord of opinion, insight, recriminations, professional disagreement, and more. Who will be the referee? Who will decide if something does or does not pass as reliable coding? As the saying goes you get ten economists in a room and you'll have ten different opinions; the same is true for software experts. Such public discourse and disagreement will do absolutely nothing to engender trust and confidence in the election process, and in fact will continue to erode confidence.

I support the findings presented in the California Legislature 2006 report: "A policy decision to require open source software for voting systems would disrupt existing voting systems without providing an immediate alternative." We must find an alternative that achieves the perceived goal advocates of open source code promote, without inducing highly unacceptable risk into the election process.

Consideration may be given to a compromise solution whereby an independent government agency, the Election Assistance Commission (EAC) supported by the National Institute of Standards and Technology (NIST), be designated as an escrow facility for all vendor software. The following procedures in principal may be considered:

- 1) Federal government scientist from NIST permanently serve as reviewers and controllers of such code on behalf of the American people;
- 2) All vendor software (source and compiled) tested and certified by the Independent Testing Authorities be delivered directly to the EAC;
- 3) Rigorous configuration management controls must be in place to ensure the integrity and the accuracy of the source and compiled code;
- 4) Vendors working with the EAC, would have required software directly delivered to a specific customer – at no time once the code has left the ITAs will the vendor have possession or access to that code;
- 5) Localities would take possession of application software for use in creating elections and programming machines;
- 6) EAC would conduct regular non-announced software configuration audits to localities; and
- 7) Detailed change control processes would be coordinated between vendors, ITAs, and the EAC to guarantee control of configurations.

**Thank you,**

I appreciate the opportunity to share with the Committee my thoughts on this particular matter. I am one of many voices you will hear on this and other related subjects. But as I mentioned in the beginning of my testimony, I believe all sides to this issue have a common goal we agree on. I am sure that a reasonable and acceptable compromise will be achieved to the benefit of all interested parties, but specifically the American people.

Respectfully:

Hugh J. Gallagher  
Managing Director  
Election Systems Acquisition & Management Services

---

Mr. Gallagher is a highly qualified Executive Manager, Technologist and Researcher with over 25 years' experience in technology based industries, most notably the Election Industry, to include subject matter expertise in, and research on the Help America Vote Act, and electronic voting systems and voter registration systems design, development, testing, certification, acquisition, implementation and training.

- Master of General Administration in Information Systems Technology and Marketing;
- Bachelor of Science in Business Administration & Economics;
- Over 10 years experience in the Elections Industry;
- Managing Director and founder of Election Systems Acquisition & Management Services;
- He is a certified internal ISO 9000 auditor;
- Designed and introduced a new Direct Record Electronic (DRE) voting system product which was the first in the industry to received dual certification from Federal testing and approval bodies;
- Developed all user-required product policies and procedures, training programs, logistics plans, security plans, configuration management plans, and QC plans for the implementation of the DRE voting system;
- Currently working with the Commonwealth of Virginia on design and implementation of its' new voter registration system – in particular in the redesign of associated workflow processes to implement required Federal and state legislation as it relates to absentee voting with particular focus on UOCAVA voters;
- Instructor for the Certified Elections/Registration Administrator (CERA) professional education program conducted jointly through the Election Center and Auburn University – instruct Module IV, Information Management & Technology in Elections & Voter Registration;
- Invited speaker on voting system and election policy issues at national and state conferences;
- Invited speaker at EAC public hearings on wireless voting system technologies (CALTECH);
- Worked with disabled community regarding accessibility issues for voting systems;
- Former U.S. Naval Officer;
- Research and Publications include: "Voting System Vendor and System Comparison," 2004; "Virginia Electoral Board Member Duties and Responsibility Handbook," 2004