

Alan Dechert

From: "Robert Kibrick" <bob@verifiedvoting.org>
To: "Alan Dechert" <alan@openvotingconsortium.org>
Sent: Sunday, March 26, 2006 10:49 PM
Attach: itaa322.pdf
Subject: my comments re: the ITAA letter opposing AB 2097

Alan,

Here are my comments re: the ITAA's letter opposing California Assembly Bill 2097.

Best regards,

Bob

Bob Kibrick
Legislative Analyst, VerifiedVoting.org

1. "Our opposition to the bill stems from the proposal's impracticality **as a new standard in government procurement policy...**"

This bill does not attempt to establish a new standard in government procurement policy. Rather, it updates government policy pertaining to the certification of voting systems, period.

2. "The United States Government opposes public sector procurement restrictions giving preference to then open source development model or creating barriers to the acquisition of commercial software."

Commercial voting systems software is quite unlike most commercial software, in that it is only used in a very specific and restrictive environment (i.e., public elections) and on very specialized hardware; it cannot be acquired by California counties unless it has completed a lengthy and extensive federal and state certification process, a barrier to acquisition that is not faced by most other commercial software. The requirements (both federal and state) with which voting systems software has had to comply have increased significantly as a result of federal (e.g., HAVA) and State legislation (e.g., SB 1438) enacted during the past several years. Like such legislation, AB 2097 simply adds to list of requirements that such software must already comply to obtain certification from the State.

3. "The bill will lead to deterioration in voting systems procurement practices and decisions...[V]oting systems acquisitions may depend ... on issues of cost, quality, qualification to federal guidelines, software performance or function, security requirements, or a universe of other factors that may lead a customer to prefer a certain type of system. A blanket policy, such as a mandate for open source or disclosed source software, can never capture these many nuances and can never allow a competent voting systems buyer to effectively weigh all factors."

Many blanket policies (i.e., requirements for disability access) are already part of the qualification process for federal and state certification, and such requirements do not prevent "competent voting systems buyers to effectively weigh all factors". Such buyers can still evaluate factors such as cost, quality, performance, and function from among competing systems that

meet established federal and state requirements -- requirements that will inevitably change over time.

4. "This bill will impose on voting system vendors to the State of California a procurement policy that will essentially strip them of their core software assets, intellectual property that has taken years and millions of dollars to develop."

AB 2097 does no such thing. Vendors still retain trademark, copyright, and patent protections for those core software assets. And unlike other commercial software (especially general purpose software designed to run on commodity hardware), voting system software cannot be readily duplicated to generate bootleg copies and sold via clandestine channels for hidden use because:

- a. Voting system software cannot be sold to counties until it has completed the federal and state certification process,
- b. Voting system software (in most cases) cannot be run on commodity hardware but only on hardware that is specific to the vendor that developed the software,
- c. The sale of voting system software is a highly-public process, typically involving numerous and well-publicized public hearings and votes of public legislative bodies (e.g., county boards of supervisors).

Given the highly-public and restrictive nature of the procurement process for voting systems acquisitions, the notion that disclosure of a vendor's source code for voting system software would enable a competitor to secretly appropriate that code and sell it to other counties without the knowledge of the original vendor appears ridiculous. And if a competitor were so brazen to attempt such appropriation and duplication, the end product would most likely be useless without the original vendor's hardware. Such brazen actions by a competitor would be clearly visible to the original vendor (due to the highly-public nature of the voting systems procurement process), who could still bring prosecution for trademark, copyright, and (where applicable) patent infringement.

5. The ITAA letter makes note of the deficiencies (i.e., a requirement to disclose third-party code) in a specific bill in North Carolina. However, the disclosure requirements in AB 2097 make an explicit exemption for third-party COTS software.

6. "Review of system source code by technical and elections laypersons (sic) operating outside the election environment, with no ability to provide regulated feedback into the State's election management process, will not increase the quality or security of voting systems software."

The letter provides no substantiation whatsoever for this bold assertion. Furthermore, §§2(e)(2) and 2(e)(3) of AB 2097 require the Secretary of State to establish and maintain a web site that provides:

"(2) A system for acquiring and processing input from the voting public" and "(3) A reporting system to inform the public on findings, problems reports, problem resolution, and comments from the Secretary of State, the public, and vendors."

7. "... the discovery through public review of any software anomalies in the final weeks leading up to an election [would make] an almost unmanageable situation."

Such an unmanageable situation could already occur even in the absence of passage of AB 2097, since existing pre-election testing (e.g., logic and accuracy testing) is supposed to be a publicly-observable process, and such testing can discover such anomalies "in the final weeks leading up

to an election". In such situations, counties and the State are indeed faced with hard choices, regardless of whether or not AB 2097 is passed.

Is the ITAA advocating that any such voting systems anomalies that are discovered by whatever means in the "final weeks leading up to an election" should be concealed from the public?

8. "The security requirements necessary for an electronic voting systems are particularly unforgiving, with the need to eliminate, not merely detect, the possibility of compromise. The experience to date with open source software does not provide much basis for evaluating the ability of the open source model to meet these requirements."

While the first of these two sentences is certainly true, the second is debatable. However, the experience to date with "closed source" (i.e., proprietary software) provides considerable "basis for evaluating the ability of [that] model to meet these requirements"; in fact, that "closed source" model has been demonstrated (e.g., the "Husti Hack") to fail rather miserably in meeting those requirements, even by such "closed source" software that has completed both the federal and state certification process.

9. "The Secretary, or other authority, should then seek solutions that address those threats [to voting systems] and challenge those solutions until it seems clear that the solution being adopted has strong advantages over other possible solutions... To leap to a single proposed approach, without evaluating other possible approaches, would do the State and its citizens a disservice".

It is noteworthy that the ITAA failed to suggest even a single alternative solution.
