



SHARTSIS FRIESE LLP

One Maritime Plaza ♦ Eighteenth Floor
San Francisco, California 94111-3598

Robert C. Friese
rfriese@sflaw.com
(415) 773-7244

October 6, 2006

VIA HAND DELIVERY, EMAIL, FACSIMILE, & U.S. MAIL

Members of the Alameda County Board of Supervisors
Nancy E. Fenton, Esq.
Deputy County Counsel
County of Alameda
County Counsel's Office
1221 Oak Street, Suite 450
Oakland, CA 94612-4296

Re: Vulnerability Assessment of Sequoia Voting Systems

Dear Members of the Alameda County Board of Supervisors and Ms. Fenton:

I write regarding the October 4, 2006 Pacific Design Engineering report entitled "Sequoia Voting Systems Vulnerability Assessment and Practical Countermeasure Development for Alameda County," (the "Report") and the Registrar of Voters' recommendation that the Report be "received by the Board of Supervisors" at its October 10, 2006 meeting. While we believe that the Report represents a significant step in the right direction, it appears that the scope of the Report is limited such that it does not reflect that the "independent security vulnerability testing" required by the Board of Supervisors at its June 8, 2006 meeting was conducted.

First, I would like to clarify a point of apparent confusion with regard to the purposes of our October 3, 2006 Petition. Petitioners do not seek to block the County's use of the Sequoia machines in the November general election, or to otherwise interfere with that election. To the contrary, Petitioners' intention is to promote the smooth, secure, and fair conduct of the November election and future elections, working cooperatively with the County to the extent possible. We recognize that it is not possible to address all of the issues presented by the Petition with only a month until the election. To the extent that the press has labeled our action as one to "block" the election, it is a mischaracterization.

Next, we are unclear about what the Registrar of Voters is asking the Board of Supervisors to do at its October 10, 2006 meeting. If, by recommending that the Report be "received by the Board," Mr. MacDonald is formally presenting the Report to the board for its due consideration, we fully support his recommendation. However, we are concerned that Mr. MacDonald is recommending that the Board accept and approve the Report as fulfilling the

Board's directive that the County conduct independent security vulnerability testing before making payment under the June 2006 agreement with Sequoia. Such approval by the Board at this time could only constitute a "rubber stamp" acceptance of the Report, without regard to its merits. We strongly urge the Board not to rush to an unnecessary and ill-considered determination at this time.

Simply put, the Board has not had the time to review and understand the merits of the Report. We understand from Ms. Fenton that the Board received the Report at 4:00 p.m. on October 5, at which time the Report was also made public. By providing the Board with the Report just two business days before its October 10 meeting, the Registrar of Voters has not given the Board the chance to understand what, if any, testing was conducted, what was not done, or what are the relevant standards. Most likely, the Board members will only have done an initial review of the Report, and will have an accordingly shallow understanding of its contents. The Board does not need to rush to a determination of the sufficiency of the Report, and it should not do so without a considered and thorough understanding.

More importantly, even an initial, cursory review of the Report should raise a number of important questions. Based on our initial review, Petitioners believe the Report reveals that appropriate testing of the Sequoia machines was not performed. At a minimum, the Report does not contain enough information for the Board to conclude that adequate testing was performed. Because of this, if the Board acts upon the Report at all at its October 10 meeting, it should require the Registrar of Voters to amend or supplement the Report with additional information that will allow the Board to reach an informed decision.

The assessment issued by PDE is useful in that it identifies vulnerabilities in Alameda County's configuration of its voting system. For example, suggestions that the County add antivirus software, firewalls, and checksums are useful. They will help to make the systems less insecure to outsider attack, and are well taken. However, the assessment fails to meet the requirement of the Supervisors' amendment of June 8 for various reasons, including the following:

- **No Testing of Sequoia Equipment was Performed:** Critically, the Report does not reflect any actual testing of Sequoia equipment. No Hursti-type "hack test" or "red team" testing was performed. The "Methodology" section (pages 1-4), which purports to describe three areas of analysis, reflects that the Electronic Voting System Architecture was analyzed only via "interviews with Sequoia Systems staff," (page 3); Vote Count Room Security was assessed through interviews, a physical inspection, and an automated security software scan (pages 3-4); Electronic Voting System Process was assessed through interviews with county election official and reviews of related documentation (page 4).
- **The Report Is Not Independent:** As indicated throughout the Report, PDE relied on interviews with Sequoia representatives and County election officials. All of these groups of people, but especially Sequoia, have an interest in a finding that the Sequoia

machines are secure. Reliance on the vendor for information about its own equipment is inconsistent with independent testing. The Report and the procedures reflected therein do not comply with the Board of Supervisors mandate that the testing was to be performed in an independent manner.

- **The Comparisons To Diebold Are Gratuitous:** The Board of Supervisors did not ask for a comparison of Sequoia systems with Diebold systems. They asked for security testing of Sequoia systems. Such comparison tables may be acceptable when issued by Sequoia's marketing department, because readers know that they must be taken with a grain of salt. They are not acceptable in a supposedly independent study, particularly when they are not supported by specific evidence.
 - **The Comparisons To Diebold Are Misleading:** The comparisons to Diebold misleadingly focus the Board's attention on vulnerabilities known about Diebold equipment, but ignore many of the vulnerabilities suspected about Sequoia (e.g., the Compuware report commissioned by the State of Ohio).
 - **The Comparisons To Diebold Are Unsupported:** The comparisons in the Report claim that Sequoia is not vulnerable to many of the listed attacks, but provide no basis for the claims. Because no Hursti-style security testing has been performed on the Sequoia equipment, there is no reason to believe these unsupported claims about the Sequoia equipment. (Indeed, the only reason Diebold's vulnerabilities are known is because the type of testing sought by Petitioners was performed on the Diebold equipment.)
- **Ignores Attacks From Insiders:** The Report ignores the greatest security threats, which are from insiders, particularly company insiders. Sequoia insiders, who are subject to bribery, blackmail, or overzealous political motivation, have extensive access to plant hidden, malicious code in the software or firmware of the voting system. Indeed, the Report recognizes that "an attacker must not gain unauthorized access the inside of the scanner" (page 10). Also, "attacks could be initiated against the high-speed optical scanners, ..., the tally servers, or network infrastructure devices" (page 9). Yet the Report does not discuss in any professional manner the problem of insiders attacking the system. This cannot be called a complete assessment of the whole system.
- **Ignores Known Threats to Windows Systems:** The Report glosses over a major threat to the central Windows-based systems, the loading, particularly shortly before an election, of "patches from Windows and 3rd party vendors" (page 11). All software patches, including Windows patches, are potentially unsafe. Installing them without additional security testing assumes that their authors have no vested interest in the outcome of an election. This assumption is dangerous, yet the Report fails to address it.

- **Report Makes False Claims:** The Report contains statements that are known by people with sufficient expertise in the area to be inaccurate or misleading. Such statements include:
 - Claim that Sequoia has no known software bugs (page ii): It is universally recognized that all complex software has bugs.
 - Claim that the precinct and central voting systems are not subject to malicious code insertion (pages ii, iv, 11): All software is vulnerable to malicious code insertion, whether from internal or external sources. And, systems that run on Windows, such as the Sequoia central systems, are especially vulnerable to external attacks.
- **Pacific Design Engineering May Not Be Qualified To Test Election Equipment:** The Report does not provide evidence of PDE's expertise or qualifications in the area of elections systems security testing. In the absence of such evidence, and from a review of PDE's website, we can only conclude that PDE is a provider of business-to-business information technology systems services.
- **Pacific Design Engineering Is Not Qualified To Assess Election Procedures:** Moreover, the Report purports to assess election security matters that have little to do with information technologies. This, for example PDE refers to the audits of 1% of precincts as helping to make the systems secure. There is no reason to believe that PDE is qualified to render a professional opinion on the adequacy of the audit procedure as a means of identifying discrepancies caused by error or tampering. Indeed, a 1% audit is statistically inadequate, especially if the paper trail created by the elections equipment does not allow for a well-executed audit.
- **The Report Is Too Narrow To Respond To The Board's Directive:** The Report is about Alameda county, not Sequoia voting system hardware and software: "Our charter for this engagement is thus restricted to practical countermeasures that can actually be implemented by Alameda County" (page 19). This means that PDE ignored things the County is powerless to act on: the software on the systems, hidden code, and hardware vulnerabilities that only Sequoia, if anyone, could correct, steps that by law would in any event require months of advance notice to permit renewed federal and state testing and certification.

Because PDE artificially restricts its "charter"—a restriction found nowhere in the Board's directive—the PDE Report can fairly support only the following claim: Given that PDE (1) was not asked or allowed to examine Sequoia software code or conduct actual security testing on Sequoia hardware or software; (2) relied on representations by Sequoia about its equipment; and (3) did not consider countermeasures that it deemed "impractical" or beyond Alameda County's capability to implement, PDE can only claim that certain aspects of the Sequoia system appear to be reasonably secure. This conclusion is not an answer to the question the Supervisors asked, nor is it an answer that

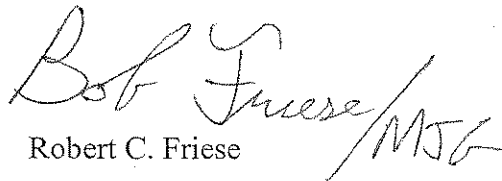
should inspire any confidence on the part of the Supervisors or the voters that their election system is secure.

In sum, while Petitioners have serious concerns that "independent security vulnerability testing" was not conducted, at a minimum we urge the Board to decline to find at this time that the Report satisfies the Board's conditions regarding security testing. The Report simply does not contain enough information to support such a finding, and the Board has not had enough time to reach such a conclusion. Instead, the Board should take the Report under consideration at this time.

The County Registrar of Voters and the Board of Supervisors now have the opportunity to give the voters a system in which they can have confidence (and which could possibly serve as a model elsewhere), or they can lock in place a flawed system--one quite possibly difficult to change once approved and paid for. Given the many important questions unanswered, and not asked, in the Report, it would be strange and disappointing to accept this result. Or the County can choose to do the job it appears was sought and voted for at the Board's hearing of June 8, 2006. The choice seems easy, and the Board could only ignore the constructive path suggested in the comments above through a lack of understanding of the technology and the consequences of not taking the next step.

We respectfully request that the Board not approve the Report until the issues we identify have been addressed competently, independently and in writing. We do not seek to interfere with the coming election, and are willing to work toward a solution which makes the prospective court hearing anticipated for mid-November unnecessary. We ask only that our clients and the full body of voters in Alameda County be given the chance.

Sincerely yours,

A handwritten signature in cursive script that reads "Bob Friese" followed by a stylized flourish that appears to be "MSG".

Robert C. Friese