results from an actual count of 6 "No" votes and 2 "Yes" votes to a reported, and inaccurate, count of 7 "Yes" votes and 1 "No" vote.

94. On or about December 20, 2005, Secretary of State McPherson issued a press release calling for additional testing of the Diebold Voting System. In the press release, McPherson stated that "[d]uring a thorough review of the application for the Diebold system currently pending certification, we have determined that there is sufficient cause for additional federal evaluation." A true and correct copy of the press release is included in the Appendix as Exhibit 14.

95. On information and belief, the Secretary of State's decision was based, in part, on the flaws revealed by Hursti's successful manipulation of the Diebold systems in Florida.

96. Also, on December 20, 2005, the Chief of the Secretary of State's Elections Division sent a letter to Diebold requesting that it submit source code contained on the memory cards used with the AV-OS and AV-TSx for further federal testing due to security concerns:

> Unresolved significant security concerns exist with respect to the memory card used to program and configure the AccuVote-OS and the AccuVote-TSX components of this system because this component was not subject to federal source code review and evaluation by the Independent Testing Authorities (ITA) who examined your system for federal qualification. It is the Secretary of State's position that the source code for the Accubasic code on these cards, as well as for the Accubasic interpreter that interprets this code, should have been federally reviewed.
>
> *****
>
> . . . .Therefore we are requesting that you submit the source code relating to the Accubasic code on the memory cards and the Accubasic interpreter to the ITA for immediate evaluation.
>
> *****
>
> *We require this additional review before proceeding with further consideration of your application for certification in California.* Once we have received a report from the federal ITA adequately analyzing this source code, in addition to the technical and operational specifications relating to the memory card and interpreter, we will expeditiously proceed with our comprehensive review of your application. (emphasis added)

A true and correct copy of the December 20, 2005, letter is included in the Appendix as Exhibit 15.

C. The Secretary Of State Requests Review Of The Diebold Voting System's Memory Cards By Members Of His Voting Systems Technology Assessment Advisory Board And Their Analysis Confirms The Existence Of Known Security Flaws And Discovers Others.

97. In or about this same period, the Secretary of State also asked members of the Voting Systems Technology Assessment Advisory Board ("VSTAAB"), an expert panel the Secretary of State's office created to help assess voting technology, to perform additional security testing of the Diebold Voting System's memory cards.

98. The panel had access to the AV-TSx source code for a period of four weeks.

1. The VSTAAB Security Analysis.

99. On or about February 14, 2006, three computer scientist members of the VSTAAB from the University of California issued a report entitled "Security Analysis of the Diebold AccuBasic Interpreter" (the "VSTAAB Report"). A true and correct copy of the VSTAAB Report is included in the Appendix as Exhibit 16.

100. The VSTAAB Report noted that the AV-TSx "had not been subjected to thorough testing and review by" the national ITA which had approved the system in 2005. Ex. 16 at 1.

101. The VSTAAB Report confirmed that the AV-TSx's software architecture, in particular its AccuBasic language and interpreter, contained "interpreted code" in violation of the Federal Election Commission's 2002 Voluntary Voting System Standards. *Id.* at 35. Compliance with these standards is mandatory under California law. Elec. Code §§19250 (a-b), 19251(d).

102. The VSTAAB Report also confirmed Harri Hursti's finding that the AccuBasic script used in the memory cards of the AV-OS (and AV-TSx) can be replaced with malicious script that would allow an attacker to tamper with vote counts and reports and then conceal that the tampering had taken place. Ex. 16 at 18-19. The Report found that the AV-TSx had the same vulnerabilities as the AV-OS. *See id.* at 2 (noting that "[a] majority of the bugs" in the Diebold optical scan system were also present in the AV-TSx system), 19 ("The

AV-TSx also appears to be at risk for similar attacks."). While the Report noted that the AV-TSx contained a "potential" protection against hacking not present in the AV-OS, it also noted that this protection was only "potential," not actual, because the AV-TSx cryptographic protection contains a "serious flaw." *Id.* at 2-3.

103. The VSTAAB Report also described a number of previously undiscovered and/or unreported "serious vulnerabilities" in the AccuBasic interpreters for both the AV-OS and AV-TSx machines that could be exploited by an attacker with unsupervised access to a memory card to modify vote totals, or otherwise compromise the integrity of an election. *Id.* at 11-18. Critically, these bugs would not be detected by any amount of functionality testing. *Id.* at 2.

104. The VSTAAB Report noted that the AccuBasic interpreter appears to have been written with commercial standards of software development, rather than the high-assurance standards that one would expect for an application where security was of utmost importance. *Id.* at 23.

2. The VSTAAB's Recommended "Mitigation" Measures.

105. After outlining the security vulnerabilities they discovered, the authors of the VSTAAB Report recommended some possible mitigation measures. The authors divided their discussion into two categories of mitigation strategy—short-term and long-term.

106. As a *short-term* mitigation strategy, the VSTAAB Report recommended implementing procedural and physical safeguards to protect the Diebold machines and memory cards from tampering. The suggested *short-term* safeguards included updating the cryptographic keys on every AV-TSx machine, and certain physical security measures including chain of custody control of memory cards and the use of tamper-evident seals (ideally applied to seal the memory cards into voting system units at a central warehouse in advance of the election and not removed until the units were back in the control of county officials). The VSTAAB Report states that "[w]hile these strategies do not completely eliminate all risk, we expect they would be capable of reducing the risk *to a level that is*

manageable for local elections in the short term." Ex. 16 at 36 (emphasis added). The recommended short-term strategies did not include any modification of source code, because of the time it would take time to perform the additional coding and to secure federal qualification and state certification of the code changes.

107. By contrast, according to the authors, "[i]n the longer term, or for statewide elections, the risks of not fixing the vulnerabilities in the AccuBasic interpreter become more pronounced. Larger elections, such as a statewide election, provide a greater incentive to hack the election and heighten the stakes . . . . For statewide elections, or looking farther into the future, it would be far preferable to fix the vulnerabilities discussed in this report." *Id.* at 36-37 (emphasis added).

108. The VSTAAB Report's recommended long-term mitigation measures primarily consisted of changing the Diebold machines' software and or hardware including: (1) revising the source code of the AccuBasic interpreter to fix the bugs identified in the Report and to incorporate defensive programming practices, including the elimination of all "trust" in the memory card (*i.e.* eliminate any implicit assumption that the memory card could not be tampered with); (2) protecting the AccuBasic code from tampering by embedding it in non-removable storage and/or protecting it with cryptography; (3) changing the architecture of the AV-OS and AV-TSx so they do not store code on removable memory cards; and (4) changing the architecture of the AV-OS and AV-TSx to eliminate all interpreted code and bring them into compliance with the federal voluntary standards. *Id.* at 31-36.

3. The VSTAAB Report Acknowledges Its Limited Scope And The Existence Of Other Security Issues.

109. The VSTAAB Report also made clear that the scope of the review the Board was allowed to perform was very limited. For example, the VSTAAB investigators limited their review to Diebold's proprietary AccuBasic scripting language which Hursti had demonstrated was problematic. Ex. 16 at 6. In addition, the VSTAAB Report did not examine the source code for the GEMS election management system, even though the

investigators noted that "[i]t is widely acknowledged that a malicious person with unsupervised access to GEMS, even without knowing the passwords, can compromise GEMS and the election it controls." *Id.*

110. The VSTAAB Report's authors "did not have access to a genuine running system." *Id.* at 8. Their analysis was based only on a "stubbed-out version of the code," but even with this piece they were able to confirm that "one of the attacks we discovered (the only one that we tried) actually works." *Id.*

111. Finally, the VSTAAB Report assumed that the hypothetical person seeking to alter ballot results did not have any inside confederates, or access to passwords or cryptographic keys. *Id.* at 7. In short, the VSTAAB Report discovered numerous security flaws in the very limited area of the Diebold Voting System software that it examined—the system's memory cards—but did not exclude the possibility, and in fact acknowledged the likelihood, that significant additional security flaws existed in other parts of the Voting System.

D. The Diebold AV-TSx's Paper Audit Trail System Has Not Been Shown To Meet State Requirements.

112. California law requires that DREs produce an "accessible voter verified paper audit trail." Elec. Code §19250(a-b). The Legislature imposed this requirement to protect against programming error or fraud.

113. In an attempt to meet California's requirement for a voter verified paper audit trail, the current version of the AV-TSx comes with an attached printer, the AccuView Printer Module. The printer module produces a record of the voter's vote on a continuous roll of thermal paper which fully-sighted voters are supposed to be able to view through a small window and then accept or reject the record as correct. If the voter rejects the record as incorrect, the printer is to make a mark on the paper roll at the bottom of the particular entry, but the record is not removed from the roll. All paper records, including the rejected votes and provisional votes, are spooled into a sealed canister inside the machine.

1. The AV-TSx And Its Attached Printer Destroy Vote Records And Experience Frequent Crashes During Testing By California Elections Officials In 2005.

114. On July 20, 2005, the Secretary of State's office oversaw a "volume test" of the AV-TSx's attached printers. The volume test was performed at a warehouse supplied by the San Joaquin County Elections Department. November 14, 2005, Staff Review and Analysis at 8. A true and correct copy of the November 14, 2005, report is included in the Appendix as Exhibit 17. Most of the testers were election staff from various counties. *Id.* at 8.

115. The July 20, 2005, test revealed critical flaws in the hardware and software of the AV-TSx. The system destroyed or lost paper audit records, a problem which would complicate manual recounts. Ex. 11 at 6. The AV-TSx also experienced ongoing software failures, making it "possible that votes could be lost or corrupted." *Id.* at 7.

116. In a July 27, 2005 letter, the Secretary of State rejected Diebold's then-pending application, noting that "[i]n the course of testing your system, my staff has noted problems with paper jamming on the AccuView printer module. Additionally, my staff has noted an additional recurring problem with the AccuVote-TSX that freezes the ballot station and requires it to be rebooted. After extensive testing, these problems remain unresolved." A true and correct copy of the July 27, 2005 letter is included in the Appendix as Exhibit 18.

117. An October 11, 2005 report by the VSTAAB describing the test and its results concluded that "any system with failure rates this high is not ready for use in an election." Ex. 11 at 5.

118. In the weeks between the Secretary of State's July 2005 rejection of the AV-TSx application and the October 2005 VSTAAB report, Diebold renewed its application for the AV-TSx.

119. As a result of this renewed application, another volume test was held on September 28, 2005, in San Diego. Ex. 17 at 9. However, instead of County Elections Officials, this time the test was staffed by "[t]emporary workers contracted by the Secretary of State." *Id.*

120. This second test was conducted under close supervision of Diebold staff who

conducted "[s]upport operations," including "programming the voter activation cards." *Id.* There is no indication that any of the VSTAAB experts who witnessed the first test were present at the second test. As such, although the Secretary of State's November 14, 2005, staff report on the test stated that none of the errors experienced during the second test "resulted in the loss of the record of a vote," (*id.* at 10) this test lacked scrutiny and verification by any independent experts. The ability of the AV-TSx's printers to function when operated by County Elections Officials under the pressure of a statewide California election therefore remains unknown.

2. The Secretary Of State's Staff Report Confirms That The Diebold TSx's AccuView Printers Do Not Comply With Federal And State Accessibility Requirements.

121. The Secretary of State's November 11, 2005, consultant's report ("Freeman Report") on the AV-TSx system discussed the question of the Diebold TSx AccuView Printer modules' compliance with Help America Vote Act ("HAVA") and state law requirements for equal access to disabled voters. Ex. 13 at 8. The Freeman Report noted that the system "does not provide a blind voter with the opportunity to verify the vote using the paper audit record." *Id.* Non-visual confirmation of the paper record is required under state law. Elec. Code §§19250(a-b), 19251(a).

122. The Secretary of State's November 11, 2005, consultant's report on the AV-TSx system disclosed that the AV-TSx "does not provide support for assistive devices for the physically disabled such as sip and puff or jelly buttons." Ex. 13 at 12. Such devices are necessary to provide access to low-mobility and low-dexterity voters.

3. The Secretary Of State Failed To Examine Whether The AV-TSx Thermal Paper Roll Records Can Meet California Mandatory Audit And Recount Requirements.

123. On information and belief, none of the Secretary of State's tests of the AV-TSx analyzed, or purported to analyze, whether the thermal paper roll records produced by the AV-TSx's attached printer were capable of supporting a manual audit. State law requires a

manual audit of at least 1% of the precincts in an election. Elec. Code §15360.

124. State law also requires that DRE machines produce a "paper record copy" of every vote. Elec. Code §19250(d). Elections Code Section 19251(e) defines "paper record copy" as "an auditable document printed by a voter verified paper audit trail component that corresponds to the voter's electronic vote and lists the contests on the ballot and the voter's selections for those contests."

125. This failure to test or certify for capacity to withstand a manual audit is troubling given the Secretary of State's own admission, in a September 9, 2005, opinion piece for the San Jose Mercury News, that "[u]sing paper receipts as secondary ballots at this point is too risky. They are designed for the voter's review and are not printed on ballot-quality paper and might not retain their quality during the often-lengthy recount and legal challenge periods." A true and correct copy of the opinion piece is included in the Appendix as Exhibit 19.

126. The California Association of Clerks and Election Officials has also questioned whether paper records generated by DREs are suitable for a manual audit. In a September 1, 2005, letter to the governor, the association noted several reasons why DRE paper records would make it "extremely problematic" to conduct precinct-specific 1% manual recounts as required by Elections Code Section 15360. Those reasons include the following:

(a) eligible provisional ballots would be "indistinguishable from the ineligible ballots due to the inability to identify which records represent the eligible and/or ineligible images";

(b) because early voters can vote outside their precinct, early voters from multiple precincts may have their votes on a single DRE, making it "onerous and time consuming, if not impossible" to determine which votes are associated with a particular precinct;

(c) potential mechanical problems, including printer jams and illegible print;

(d) because the paper record is in the voters' chosen language, "[t]ranslation . . . for the purposes of performing the 1% manual tally will be difficult and