



SCHOOL OF INFORMATION
102 SOUTH HALL # 4600
BERKELEY, CALIFORNIA 94720-4600
(510) 642-1464
(510) 642-5814 Fax

Aaron Burstein
Joseph Lorenzo Hall
School of Information
102 South Hall
University of California, Berkeley
Berkeley, CA 94720-4600
p: 510.759.1597
f: 815.301.3881

November 5, 2009

Mr. Brian Hancock
Director of Voting System Testing and Certification
Election Assistance Commission
1225 New York Avenue, NW
Suite 1100
Washington, DC

Dear Mr. Hancock,

Thank you for your reply of October 21, 2009, to our letter of October 13, 2009. We appreciate your pointing out that relevant documents are available on the EAC's website. Of course, it was the EAC's commendable policy of making these documents publicly available that allowed us to initiate this dialogue. As you know, neither test plans nor test reports were available under the NASED qualification testing program; this change is important for establishing a more trustworthy voting system testing and certification program under the EAC.

After carefully reviewing your letter, however, we continue to question whether iBeta's test plan for the Premier system fully incorporates some of the lessons of the California Top-to-Bottom Review (TTBR) into EAC testing and certification. Even for the examples the EAC points to in its reply, the test plan does not state in sufficient detail what iBeta proposed to do to test the system. For example, an element of the security test—"port access is controlled" (test plan p. 73)—states a desired result or conclusion but does not describe how iBeta would arrive at that conclusion nor under what conditions would this element fail.

Moreover, our letter was not limited to the red team report; our concerns about applying the lessons of the TTBR extend to the source code and document reviews, too.¹ With respect to security, the source code review contained numerous vulnerability reports, some of which are best addressed during system development and/or testing and certification. These vulnerabilities are often exceedingly difficult to mitigate in the context of a live election environment. We would expect to see evidence in the test report that, for example, "Issue 5.2.4 from the CA TTBR report on the Diebold/Premier voting system—

¹Recall that there were four elements to the TTBR: red team review, source code review, document review and accessibility review. Each of the ten TTBR reports are available at: http://www.sos.ca.gov/elections/elections_vsr.htm.

‘Setting a jumper on the motherboard enables a bootloader menu that allows the user to extract or tamper with the contents of the internal flash memory’—has been corrected by [*some modification of the system*]’. As it stands now, neither the public nor election officials have any basis for confidence that these issues have been addressed.

One of the central findings from each of the separate TTBR document reviews was that the testing and certification documentation, especially with respect to security properties, was not sufficient to understand how these systems are tested. In the present case of the Assure 1.2 system, neither the main test report nor its attachments state in sufficient detail what iBeta actually did during its tests. The main report provides an overview of iBeta’s security testing procedures and its criteria for acceptance/rejection under 2002 VSS requirements. The appendix to the test report simply repeats statements from the test plan. Nowhere is there sufficient detail one could use to replicate the testing performed by either VSTL (SysTest and then iBeta), to evaluate the particular testing techniques used by the VSTLs, or, specifically, to validate that the system has been modified to fix any of the concerns raised by the TTBR.

Finally, you note that iBeta tested a voting system that was a more recent version than the one that was examined during the TTBR. This fact, by itself, has little bearing on whether the TTBR findings are applicable. Without access to the voting system and its source code as well as the specific test suites and procedures used by the VSTL, it is impossible to determine whether iBeta’s test plan would have addressed all issues raised by the TTBR. Clearly, the EAC believed that the TTBR was potentially relevant to the updated system, as was evident from its directing iBeta to assess whether its test plan covered all issues raised by the TTBR.

In summary, the test plan and test report, taken together, do not demonstrate how iBeta’s tests covered the issues raised by the TTBR. The EAC has done a great service by making these documents available, but the substance of the documents falls short of assuring us that iBeta’s tests covered the TTBR’s findings.

Sincerely,

Aaron Burstein
Joseph Lorenzo Hall

CC: Senator Charles Schumer, Chairman, U.S. Senate Rules and Administration Committee
Senator Robert Bennett, Ranking Member, U.S. Senate Rules and Administration Committee
Congressman Robert Brady, Chairman, U.S. House Committee on House Administration
Congressman Dan Lungren, Ranking Member, U.S. House Committee on House Administration
Commissioner Gineen Bresso Beach, Chair, U.S. Election Assistance Commission
Commissioner Donetta Davidson, Vice-Chair, U.S. Election Assistance Commission
Commissioner Gracia Hillman, Commissioner, U.S. Election Assistance Commission
Executive Director Thomas R. Wilkey, U.S. Election Assistance Commission
Secretary of State Trey Grayson, President, National Association of Secretaries of State
Secretary of State Debra Bowen, California Secretary of State
Secretary of State Jennifer Brunner, Ohio Secretary of State
Peggy Nighswonger, President, National Association of State Election Directors
Spencer Overton, Principal Dep. Asst. Attorney General, Office of Legal Policy, U.S. Department of Justice
Jon Crickenberger, Voting System Testing Program Manager, NIST/NVLAP
Carolyn Coggins, QA Director—Voting, iBeta Quality Assurance
Frank Padilla, Program Manager for Voting System Test Programs, Wyle Laboratories
Brian Phillips, President and CEO, SysTest Laboratories
Kelly A. Rohacek, ITL Practice Director, CIBER, Inc.