U.S. ELECTION ASSISTANCE COMMISSION
1225 New York Ave. NW – Suite 1100
Washington, DC 20005

October 20, 2009

Mr. Aaron Burstein
Mr. Joseph Lorenzo Hall
School of Information
University of California, Berkeley
102 South Hall #4600
Berkeley, CA 94720-4600

Dear Mr. Burstein and Mr. Hall:

Thank you for your letter (attached) dated October 13, 2009, concerning the federally accredited Voting System Test Lab's (VSTL) consideration of the California Secretary of State's Top-To-Bottom Review (TTBR) in developing the test plan for the Premier Assure 1.2 voting system.

The VSTL that tested the Premier Assure 1.2, iBeta Laboratories, closely reviewed the findings of the TTBR during the development of its test plan in accordance with the requirements of EAC's Testing and Certification program and the "Evolution of Testing" requirement contained in Section 1.5 of the 2002 Voting System Standards (VSS). In addition, the VSTL reviewed the results of the Kentucky, Ohio, and Connecticut Reports which resulted in an update of the Security Test Case to verify that Connecticut's recommended tamper-resistant seals were incorporated into the Premier Technical Data Package (TDP). The review of the 3 March 2009 California Secretary of State report was also reviewed as well as the Premier Product Advisory Notices. Finally, please note that the software and firmware versions of each component of the system reviewed by California were an earlier version than that tested by the EAC VSTL. A comparison is listed below for your information.

California TTBR Diebold GEMS 1.18.24 (CA SOS Withdrawl Notice, October 25, 2007)

1. GEMS software, version 1.18.24,
2. AccuVote-TSX with AccuView Printer Module firmware version 4.6.4,
3. AccuVote-OS (Model D) with firmware version 1.96.6,
4. AccuVote-OS Central Count with firmware version 2.0.12,
5. Vote Card Encoder, version 1.3.2,
6. Key Card Tool software, version 4.6.1, and
7. VC Programmer software, version 4.6.1.

EAC Certified Premier Assure 1.2 (EAC Certification August 6, 2009)

1. GEMS software, version 1.21.5
2. AccuVote-TSX with AccuView Printer Module firmware version 4.7.8
3. AccuVote -OS (Models A, B, C and D) with firmware version 1.96.13

4. AccuVote –OS Central Count with firmware version 2.0.15
5. Vote Card Encoder, version 1.3.3
6. Key Card Tool software, version 4.7.8,
7. VC Programmer software, version 4.7.8

During their review, iBeta concluded that all concerns contained in the report were covered by the testing proposed by the test plan and the test cases developed for that test plan as required by the federal testing and certification process. The EAC also worked with iBeta to ensure all issues contained in other applicable reports posted in the EAC's online voting systems clearinghouse were addressed. These steps ensured that all security issues raised by the TTBR were specifically addressed in iBeta's testing of the Premier Assure 1.2 system.

For example, the TTBR Red Team found that database files were not protected. The iBeta test plan version 1.0 included a test to determine if "cast ballots and vote counts are protected from tampering" and "modification of the system and application of audit log is prevented" (pg. 74). In addition, the test plan included the following specific security test methods (pg. 32):

- Attempts to bypass or defeat voting system security including: changing vote data, copying voter cards, ability to bypass user passwords, modifying data in audit logs, and accessing controlled functions without appropriate validation.
- Voter denial of service attacks introduced via the voter card or results cartridges and memory cards.
- Attempts to circumvent physical security devices without detection, including destructible seals and system components locks for cartridge and memory card slots, polls switches, keypads, and hardware components.

In another example, the TTBR Red Team identified security vulnerabilities in the GEMS audit logs. The VSTL test plan included the following related security tests:

- Physical or logical access controls on ballot preparation, vote counting, and reporting equipment.
- Password and/or token access
- Additional three-factor authentication techniques
- Port access is controlled
- Default passwords are changeable after initial login
- Minimal password strength constraints are imposed by the vendor or settable by the jurisdiction
- Audit logs cannot be modified

Other examples of issues highlighted by the TTBR that were included in the VSTL test plan include PCMCIA card/slot encryption and authentication (pg. 74), documentation review of industry standard password policies (pgs. 73 and 75), and man-in-the-middle attacks (pg. 72).

The information above can be found in the approved test plan for the Premier Assure 1.2 voting system posted to the EAC Web site on April 7, 2009. I encourage you to review the approved test report to verify the testing that was done and the results of that testing. As you are probably aware, the EAC posts to its Web site all draft and approved test plans and test reports as well as all program correspondence to keep the public fully informed of its testing and certification process.

I encourage you to review all documents on our Web site and to contact me at any time should you have concerns or questions regarding our process.

We appreciate your interest in the federal testing and certification process and your commitment to expanding knowledge of voting technology security. Sharing such information with the election community is central to ensuring the integrity of America's voting systems, and we value your contribution to it. We also commend the state of California for their leadership on this topic, and for submitting the report to us for inclusion in our online voting systems clearinghouse.

Sincerely,

Brian J. Hancock
Director of Voting System Testing and Certification Program
U.S. Election Assistance Commission

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
Mark Phillips, President, SysTest Laboratories
Kelly A. Rohacek, ITL Practice Director, CIBER, Inc.

UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

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

October 13, 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,

We write to you on behalf of those individuals listed below from the California Secretary of State's Top-To-Bottom Review (TTBR) in 2007. The TTBR was an unprecedented, in-depth evaluation of California's voting systems, which allowed investigators to gain a better understanding of their vulnerabilities.

As you know, the EAC recently certified Premier's Assure 1.2 voting system as conforming to the 2002 Voting System Standards (VSS). This system was tested by iBeta Laboratories (iBeta), one of the accredited Voting System Test Labs (VSTLs). According to the posted test plan—the roadmap for a VSTL's evaluation of a voting system during certification testing—for Premier Assure 1.2, iBeta interpreted the TTBR studies of the Premier system's predecessor to have "concluded that the vulnerabilities within the system depend almost entirely on the effectiveness of the election procedures." On the basis of this interpretation, iBeta developed a test plan that called for "no additional testing" of the Premier system's security properties. The EAC approved this plan.

Taken together, iBeta's misunderstanding of the significance of the TTBR findings and the EAC's approval of a test plan that was designed around this misunderstanding, represent a missed opportunity to use the testing and certification process to improve voting system integrity and reliability.

iBeta misunderstands the results of the TTBR. The TTBR concluded that the number, extent, and severity of these vulnerabilities were so substantial that the technological security mechanisms were completely inadequate to protect the integrity and security of both the systems and of the election.[1] This directly contradicts the statement that "the vulnerabilities within the system depend almost entirely upon the effectiveness of the election procedures." The vulnerabilities are present, regardless of the election

[1] Other studies, such as the EVEREST study that the Ohio Secretary of State sponsored, reached similar conclusions.

procedures. The team concluded that these flaws were so severe as to render the system's technological security measures essentially without value; these vulnerabilities could only be mitigated by the strictest of procedures. The California Secretary of State's response to the TTBR was to decertify two systems until their respective vendors, one of which was Diebold,[2] fixed many problems with their security mechanisms. Even now, these machines are subject to strict new procedural rules designed to mitigate the vulnerabilities which remain. Such drastic measures were necessary precisely because the underlying vulnerabilities were not detected and analyzed during conformance testing.

iBeta's light treatment of the TTBR results, therefore, should not have received the EAC's approval. If Premier sought only administrative approval of small changes to a legacy system, the approved test plan would be less of a cause for concern. iBeta's testing of the Premier system, however, was conducted under the new EAC certification program that serves as the foundation for testing under the 2005 VVSG and subsequent standards. Conformance testing under the EAC framework is one of the principal ways to detect and cure common classes of basic vulnerabilities in voting systems. The EAC should use its VSTL oversight to require test labs to conduct thorough evaluations of voting system vulnerabilities during conformance testing, so that vendors will fix vulnerabilities before systems are certified and sold.[3] When the EAC allows a VSTL to disregard important sources of information about a voting system's vulnerabilities, it weakens the testing and certification process's ability to detect and fix vulnerabilities at a relatively early stage.

We recommend that VSTLs should be required to examine each flaw and/or vulnerability described in these reports for specific systems and verify that each flaw is corrected or that specific measures are documented and recommended by the manufacturer for the voting system's maintenance and use. Many of the vulnerabilities can be corrected by relatively typical types of software modifications, the type that are routinely corrected in software that has a much shorter update schedule. For example, common buffer overflow mistakes can be corrected by range-checking variables when they are manipulated.

Of course, addressing some of the more complex vulnerabilities discovered in these studies would require significant changes to a given system's architecture. For example, vulnerabilities in how software is installed on some systems would require significant redesign in order to add authentication to the software installation functionality. In these cases, security testing should extend to the manufacturer's recommended policies and procedures. These must provide a recommended default level of physical security and careful election media handling, for example, so that a jurisdiction that follows the recommendations will mitigate the risks posed by known vulnerabilities.

If you would like to discuss this matter further, please contact Joseph Lorenzo Hall or Aaron Burstein.

Sincerely,

Aaron Burstein
Joseph Lorenzo Hall

[2] At the time of the TTBR, Diebold, Inc. had yet to change the name of its election systems subsidiary from Diebold Election Systems to Premier Election Solutions.

[3] We recognize that it is unlikely that any evaluation process will find all vulnerabilities in a system. Finding and eliminating some vulnerabilities, however, can reduce security risks. Accordingly, it is imperative that the testing and certification process uses directly relevant, readily accessible information to find vulnerabilities.

SIGNATORIES[4]

Matt Bishop *Principal Investigator*
Professor, Department of Computer Science; University of California, Davis

David Wagner *Principal Investigator*
Professor, Computer Science Division; University of California, Berkeley

Matt Blaze Associate Professor, Computer & Information Science; University of Pennsylvania

J. Alex Halderman Assistant Professor, Department of Electrical Engineering and Computer Science; University of Michigan

Candice Hoke Associate Professor of Law, Cleveland-Marshall College of Law; Cleveland State University

Richard Kemmerer Professor, Department of Computer Science; University of California, Santa Barbara

Deirdre Mulligan Assistant Professor, School of Information; University of California, Berkeley

Elliot Proebstel Department of Computer Science; University of California, Davis

Eric Rescorla Principal, RTFM, Inc.

Hovav Shacham Assistant Professor, Department of Computer Science and Engineering; University of California, San Diego

Giovanni Vigna Professor, Department of Computer Science; University of California, Santa Barbara

Dan Wallach Associate Professor, Department of Computer Science; Rice University

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.

[4]Note: Affiliations are provided for identification purposes only. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors.