UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-
OFFICE OF THE DIRECTOR

January 18, 2007

Commissioner Donetta Davidson
U.S. Election Assistance Commission
1225 New York Avenue, N.W.
Suite 1100
Washington, D.C. 20005

Dear Commissioner Davidson:

I am reporting the initial results of activities undertaken by the National Institute of Standards and Technology (NIST) relating to the evaluation of testing laboratories under Section 231 of the Help America Vote Act (HAVA). NIST has completed a comprehensive technical evaluation of the competence of two laboratories to test voting systems to Federal standards and proposes that iBeta Quality Assurance and SysTest Labs be accredited by the Election Assistance Commission (EAC) under the provisions of HAVA. We understand that the EAC will take additional steps to qualify these laboratories prior to their acceptance into the Commission's Testing and Certification Program.

NIST recognizes that transparency is key to building public trust and confidence in voting systems. To that end, we have prepared a document that explains the details of our evaluation process and addresses related questions. This document is enclosed for your reference and is also posted at http://www.vote.nist.gov. In addition, for each laboratory that NIST is proposing for EAC acceptance, we have posted our assessment report and the laboratory's detailed response to that report. These reports contain substantial detail that underlies the basis for our recommendations.

We look forward to continuing to support the EAC in its efforts to improve voting systems and the means by which they are tested and certified.

Sincerely,

William Jeffrey

William Jeffrey
Director

Enclosure

NIST

Questions and Answers About NIST Evaluation of Laboratories that Test Voting Systems

Background

The Help America Vote Act (HAVA) of 2002 directs the National Institute of Standards and Technology (NIST) to support the U.S. Election Assistance Commission (EAC) in its accreditation of laboratories qualified to conduct the testing, certification, decertification, and recertification of voting systems as provided under the act. NIST processes for carrying out this responsibility will be as open and transparent as possible to facilitate the public's understanding of how laboratories that test voting systems are evaluated.

Q. What is NIST's role in the accreditation of laboratories that test voting systems?

HAVA requires that NIST conduct an evaluation of independent, non-federal laboratories to determine their competence to test voting system hardware and software for conformance to federal standards. HAVA also specifies that NIST recommend to the EAC those laboratories that are qualified to test voting system hardware and software. The EAC will make the final decision to accredit a Voting System Testing Laboratory (VSTL) to test and certify equipment under EAC requirements.

Q. What process is NIST using to evaluate laboratories?

NIST is relying on assessments conducted by its National Voluntary Laboratory Accreditation Program as a basis for determining the competence of candidate laboratories to test voting system hardware and software for conformance to federal standards.

Laboratory accreditation is a formal recognition that a laboratory is competent to carry out specific tests. It also allows a laboratory to determine whether it is performing its work correctly and to appropriate standards.

Expert technical assessors evaluate all aspects of laboratory operation that affect the production of test data, using recognized criteria and procedures. General criteria are based on the international standard ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*, used for evaluating laboratories throughout the world. Laboratory accreditation bodies use this standard specifically to assess factors relevant to a laboratory's ability to produce precise, accurate test data, including the technical competency of staff, validity and appropriateness of test methods, and testing and quality assurance of test and calibration data. NVLAP includes this standard in NIST Handbook 150: *NVLAP Procedures and General Requirements,* available at http://www.nist.gov/nvlap.

Q. How does NVLAP determine the competency of laboratories to test voting systems?

To be accredited by NVLAP, a laboratory must demonstrate both its general technical competence and its competence to perform a core set of voting system tests. Currently, laboratories are using proprietary test methods and test cases to determine that a voting system meets existing federal standards. The federal standards are the 2002 Voting

System Standards (VSS) (see http://www.eac.gov/voting_sys_cert.htm) and EAC-adopted 2005 Voluntary Voting System Guidelines (VVSG) (see http://www.eac.gov/vvsg_intro.htm). Technical criteria for the NVLAP voting system testing laboratory accreditation program are contained in NIST Handbook 150-22: *NVLAP Voting System Testing,* available at http://www.nist.gov/nvlap.

Q. Why are laboratories using proprietary test methods?
Currently, no uniform set of tests exists to determine that a voting system meets federal standards. With the support of the EAC, in 2007 NIST will begin to develop a uniform set of non-proprietary tests to be used in conjunction with the next version of the Voluntary Voting System Guidelines (VVSG 2007). The availability and use of these open tests will improve consistency and comparability among testing laboratories.

Q. What specific tests must a laboratory meet to be judged competent?
The NVLAP assessment includes a thorough evaluation of all aspects of laboratory operation that affect the production of voting system hardware and software test data, including the adequacy of the laboratory's equipment and facilities, its system for documenting what testing is conducted, technical staff qualifications, and staff training requirements. The core of the assessment takes place during an on-site review and focuses on the laboratory's demonstrated competence to do the following:

- Review the overall system design and technical specifications for a voting system to ensure that it conforms to federal standards.
- Compare the voting system components submitted for qualification to the vendor's technical documentation (also known as a configuration audit).
- Review the "source code," the voting system's "human readable" programming instructions to verify that the code is unmodified and that settings are correct.
- Conduct an audit of the voting system's configuration to ensure that all functions work as expected and match the system's manual and other documentation.
- Test the capabilities of the voting system as a whole to ensure that it meets the requirements and that the function of any source code included in the system but not designed to meet these requirements is identified.
- Verify that the voting system reliably records votes accurately at its maximum processing volume for a specified period of time.
- Ensure that the voting system provides adequate security to prevent unauthorized access or data interception and/or disruption.

For more details on these core tests, see attachment.

Q. How long does the accreditation process take?
The accreditation process can take from nine to 18 months, including the time it takes for a laboratory to submit documentation for review by NVLAP, schedule a pre-assessment and an official on-site assessment, review assessment information from the on-site visit, and clear up any non-conformities. Laboratories that do not achieve accreditation within 12 months of their initial application must reapply to NVLAP to keep their application active.

Q. Does NVLAP conduct follow-up assessments?
Yes, to ensure continued compliance with accreditation criteria, all NVLAP-accredited laboratories undergo another onsite assessment during the first year following initial accreditation and every two years thereafter. NVLAP also can conduct monitoring visits at any time during the accreditation period; these may be unannounced.

Q. Will the names of organizations that have applied for NVLAP accreditation be made public?
NIST is maintaining a current list of applicants, along with their date of application. The list will be public and will be updated on an ongoing basis. Current and prior applicants are:
SysTest Labs, Incorporated – applied August 25, 2005 (recommended to EAC on Jan. 18, 2007)
iBeta Software Quality Assurance, L.L.C. – applied February 14, 2006 (recommended to EAC on Jan. 18, 2007)
InfoGuard Laboratories, Inc.– applied August 18, 2005
BKP Security Labs – applied December 28, 2005
Wyle Laboratories – applied August 10, 2006
Ciber, Inc. – applied September 14, 2006

Q. What documentation related to the accreditation of VSTLs is publicly available and what is not?
NIST will make publicly available non-proprietary information, including the report generated by NVLAP assessors as a result of the on-site assessment of each accredited laboratory and the laboratory responses to the on-site findings. NIST also will make publicly available the assessor checklist used during on-site assessments. By law, NIST must protect proprietary information. This includes details of a laboratory's specific testing methods and protocols.

Q. Will the EAC have access to proprietary data?
To assist the EAC in making the final decision on accrediting a Voting System Testing Laboratory (VSTL), the EAC has access to all the data, including proprietary information.

Q. Does NIST also accredit vendors of electronic voting systems?
No, NIST does not accredit vendors of electronic or other types of voting systems. The EAC has established requirements for voting system vendors and their relationship with testing laboratories, contained in its Testing and Certification Program Manual, January 2007.

Details of Core Tests Reviewed to Determine Competency of Voting Systems Testing Laboratories

1. Review the technical data package for a vendor's voting system for conformance to federal standards. This requires evaluation of:
   a. Overall system design, including subsystems, modules, and the interfaces among them.
   b. Specific functional capabilities provided by the system.
   c. Performance and design specifications.
   d. Design constraints, applicable standards, and compatibility requirements.
   e. Personnel, equipment, and facility requirements for system operation, maintenance, and logistical support.
   f. Vendor practices for assuring system quality during the system's development and subsequent maintenance.
   g. Vendor practices for managing the configuration of the system during development and for modifications to the system throughout its life cycle.

2. Conduct a physical configuration audit; that is, compare the voting system components submitted for qualification to the vendor's technical documentation. This comparison involves:
   a. Establishing a configuration baseline of the software and hardware to be tested.
   b. Confirming whether the vendor's documentation is sufficient for the user to install, validate, operate, and maintain the voting system.
   c. Examining the vendor's source code to verify that the software conforms to the vendor's specifications.
   d. Reviewing all drawings, specifications, technical data, and test data associated with the system hardware, if the software is to be run on any equipment other than a commercial off the shelf (COTS) mainframe data processing system, minicomputer, or microcomputer.
   e. Assessing user acceptance test procedures and data, based on a review of vendor documents containing this information against the system's functional specifications.
   f. Re-examining any changes to the baseline software configuration made during the course of testing. All changes to the system hardware that may produce a change in software operation are also subject to re-examination.
   g. Assessing if the voting system meets accessibility requirements.

3. Conduct a source code review, which means:
   a. Inspecting the source code to determine that the software works correctly and that there are no security glitches.
   b. Verifying that the code is unmodified and that the default configuration options have not been changed.
   c. Confirming that user selections and configuration changes are correct.

4. Conduct a functional configuration audit, which means:
    a. Verifying every system function and combination of functions cited in the vendor's documentation.
    b. Verifying the accuracy and completeness of the system's Voter Manual, Operations Procedures, Maintenance Procedures, and Diagnostic Testing Procedures.

5. Conduct a system integration test, which means:
    a. Designing and performing procedures that test the voting system capabilities for the system as a whole, to ensure that the system meets requirements defined in the VVSG 2005.
    b. Developing and implementing software test cases to be executed as part of functional testing of the system.
    c. Establishing an operational profile of the common procedures, sequencing, and options among both general system requirements and those that are specifically recognized and supported by the vendor. Any portions of the source code not covered as part of this profile must be identified.

6. Conduct reliability and accuracy tests, which means:
    a. Verifying the ability of the voting system to record votes accurately at its maximum rated processing volume for a specified period of time.
    b. Developing and implementing tests to assess voting system acceptance or rejection based on the number of relevant failures during equipment operation.
    c. Verifying the vendor's mathematical model for predicting accuracy of the voting system.

7. Conduct security tests, which means:
    a. Verifying that access control mechanisms successfully mediate read and write access to system functions and data according to system documentation.
    b. Verifying that system logs record key security functions according to system documentation.
    c. Verifying that cryptographic functions can be used according to system documentation.