Software ITA Testing to the 2002 FEC Voting System Standards

First NIST Symposium on Building Trust and Confidence in Voting Systems

National Institute of Standards and Technology

Gaithersburg, MD

December 10-11, 2003

Presented by Carolyn Coggins

SysTest labs

NASED Voting ITA Scope

NASED requires all voting systems to submit for testing by both the hardware and software ITAs.

- Hardware ITA Scope
  - Functional Testing: Polling Place
  - Environmental Hardware Testing: Polling Place (Firmware)
  - Security, Accuracy & Reliability: Polling Place
  - Accessibility: Polling Place
- Software ITA Scope
  - Functional Testing: Ballot Definition & Central Count
  - Source Code Review: Ballot Definition & Central Count
  - Documentation Review: Ballot Definition & Central Count
  - Security, Accuracy & Reliability: Ballot Definition and Central Count
  - System Level Tests: Ballot Definition Polling Place, & Central Count
- COTS exemptions:
  - Environmental Hardware Testing
  - Source Code Review

SysTest labs

Software ITA Test Standards & Resources

SysTest Labs uses the following to perform software ITA qualification testing:

- Federal Election Commission Voting System Standards published April 2002
  - Effective on voting systems submitted for test after January 8, 2003.
- SysTest Labs Quality Manual & Standard Procedures
  - Submitted to NASED as part of our accreditation
  - Documents interpretation of the VSS & software ITA test methods
  - Updated for the 2002 VSS & on-going process improvement
- Various review/report forms, data bases and templates
  - Specifically designed for testing to the requirements of the VSS
  - Assuring version control, complete documentation of review & standardized/repeatable testing.
  - Updated for on-going process improvement

SysTest labs

Physical Configuration Audit (PCA)

(FECVSS Vol. 2 Section 2, 3, 5.3, 6.6, & 6.7)

PCA Document Review of the Technical Data Package

- The reviewer the completes the **PCA Document Review Form** for each submitted document against the requirements of the VSS.
  - System Functionality, Hardware/Software/Design Specifications, Security, Training, Maintenance, User Manuals, Configuration Management and QA Program
- Documented in the **Pre-Qualification Report** sent to NASED & the vendor.

Verification of Software & Hardware Configuration

- Examine and set up the system hardware and software components for all documented components.
- Verify documentation is consistent with configuration used in the hardware ITA.

continued

SysTest labs

Physical Configuration Audit (PCA)

continued (FECVSS Vol. 2. Section 5.4)

Source Code Review

- Identify code to review (New code vs. Changed code).
- Review vendor coding standards and customize review criteria (if necessary) for the specific programming language
- Manual source code review, examine the software for:
  - Integrity- No external modification of code
    - Follow each function looking for worms, viruses or Trojan Horses
    - Check for buffer overflows that can lead to security compromise and the execution of malicious code.
  - Absolute logical correctness, modularity, overall construction, and for conformance with VSS requirements and vendor coding standards.
  - Review the system architecture for use of systems that detect intrusion.
- Automated source code review (if possible).
  - Use an automated tool to obtain metrics of the Logic Control Constructs.
  - Use security tools run to checks for constructs known to be dangerous.

SysTest labs

Functional Configuration Audit (FCA)

(FECVSS Vol. 2 Section 2, 3, 5.3, 6, 6.6, & 6.7 Appendix A)

FCA document review of the System Test & Verification Specification and all vendor testing.

- Complete the **FCA Vendor Testing Review Form** to identify test coverage of:
  - Required Ballot Preparation and Central Count Functionality
  - Optional Features
  - System Level Testing
- Document the results of the FCA Testing Review in the **Pre-qualification Report,** sent to NASED and the vendor.
  - Assess the overall adequacy of the vendor's testing
  - Identify any gaps in testing
  - Identify the scope of functional testing
  - Identify the test tasks and predecessor tasks.

SysTest labs

continued

Functional Configuration Audit (FCA)

continued (Vol. 2 Section 6, Appendix A)

Define scope of testing based upon results of FCA review

- Create the **Test Plan**, sent to NASED and the vendor
- Customize System Level Tests to the voting system
  - Voting Variations: Primary/General Election, Straight Party, Rotation, etc.
  - Security:
    - Access control policies
    - Unauthorized changes to ballot formats, cast votes, and vote totals
    - Alteration of voting system audit trails
    - Access to individual votes (maintaining ballot secrecy)
    - Test election dates 0 to 8 years out, including the presidential election cycles.
  - Accuracy & Reliability: Meets expected results for all tests over required number of votes and time
- Assess any additional risks for the specific system under test.
  - Augment tests for the specific voting system.

SysTest labs

continue

Functional Configuration Audit (FCA)

continued (Vol. 2 Section 6, Appendix C)

Test Execution:

- Observe the build of the executable from reviewed source code.
- Test environment is setup per the PCA - System Configuration.
- Execute test cases and record results
  - Any discovered issues are logged on the project Discrepancy Report.
    - Discrepancies: user documentation or claims about a system vs.actual system performance.
    - Defects: issue prevents the system from functioning correctly.
- Vendors must address all issues and resolve issues that impact qualification**.**
  - Fixes defect or discrepancy that impacts qualification.
    - Sends new code, it's reviewed, regression tested and issue is closed.
    - Decides not to support functionality or address issue with documentation. Documentation changes are reviewed, verified and issue is closed.
  - Logs a bug for a future release or chooses not to fix if it does not impact qualification.
  - All vendor responses are noted in the Qualification Report.

SysTest labs

Qualification Test Report

(Vol. 2. Appendix B)

The Qualification Test Report consists of:

- Introduction: The vendor's system, any changes and SysTest.
- Qualification Test Background: Test Process and Terms
- System Identification: System, Version, Test Environment
- System Overview: System Design and Operations
- Qualification Test Results and Recommendations: Test/Review Results, Deficiencies and Recommendation
- Appendix – Test Operations , Findings and Data Analysis:
  - Qualification Test Requirements, Source Code Review, TDP Review Summary, Test Results and Discrepancy Report
- NASED Signatory reviews and signs the report . The report's sent to the vendor and the NASED Technical Committee.
  - Committee has five days to question the report.
  - Report is revised with NASED Certification Number added.
  - Report is distributed to states or jurisdiction upon request from the vendor

SysTest labs