

## King County Elections Acceptance Testing Outline

In order to ensure that the upgraded vote tabulation System functions as documented by the Contract and provides the required security measures to ensure public trust and confidence, King County Elections has a four phase testing program. This test program is based on best practices used in other County technology projects such as the Disabled Accessible Voting Hardware project (DAVE) Contract No. Contract No. B19656B and testing practices utilized in other jurisdictions. Testing will commence upon Federal Certification of the System and Premier signing a certificate of readiness.

### I. The phases and purpose of each phase includes:

- a. Delivery Acceptance Testing of the Hardware and Software to determine if the correct model and versions of the Hardware and Software are delivered and that the Hardware, Software and System operate as Documented by the vendor.
- b. Mock Election Acceptance Testing to ensure that the Hardware, Software and System perform each of the functions required by federal, state and local election laws in order to administer an election from the beginning to the end.
- c. Volume/stress Acceptance Testing to ensure that the Hardware, Software and System will stand up to the maximum expected volume for the County's largest election as well as the System's ability to handle the unexpected such as an unanticipated peak in adjudication activity. This will be done by exercising the System with fifty percent (50%) more volume than expected and evaluating System performance. Volume/stress testing will highlight if the Hardware is properly sized in CPU capacity, System memory, etc. to meet Elections needs without crashing, unacceptable performance degradation or compromising the integrity of the System. Volume/stress testing will also provide a measurement of the System's ability to handle the inevitable growth in voter registration over the life of the System.
- d. Security review Acceptance Testing to ensure examination by third party information technology security experts beyond the federal certification process and provide confidence that any security risks are identified and mitigated.

### II. Delivery Acceptance Testing:

- a. *For All Hardware*
  1. Power on Hardware and determine that installed Software matches the Software certified in the Federal Certification process if available.
  2. Confirm that all operating System patches have been installed (unless the Contract specifically recommends against install with technically sound rationale)
  3. Confirm that anti-virus Software is up to date and run a

complete virus scan on all Systems – disable anti-virus when done (if this is still the recommended procedure by the Contract)

4. Capture System baseline configuration information on all Systems (using Windows Sysinfo, Microsoft Baseline Security Analyzer (MBSA) or other tool) into a log for future reference and confirmation that no additional Software has been added to the Systems. WA OSOS Security Survey Checklist Item SC2a requires a log of all Contract voting System Software activities.
5. Run System diagnostics on all Hardware
6. Generate hash code on all Software in the Assure 1.2 suite to be used by King County and confirm that it matches Federal Certified hash codes if available.

b. *GEMS (Global Election Management System) Election and Ballot Build Server*

1. Confirm program certificate check is active and that the certificate is the authorized certificate

c. *Access Manger Server Application*

1. Confirm program certificate check is active and that the certificate is the authorized certificate
2. Attempt to access/start Access Manger Server without proper application level permissions
3. Configure and setup users and user groups testing all combinations of permission levels and other settings
4. Test to ensure access/denial of access as expected
5. Test 2 factor authentication for all possible functions
6. Review audit log to confirm logging of user setup and security activity

d. *GEMS Tabulation Area Server*

1. Ensure server is hardened to maximum extent possible consistent with Software.
2. Confirm program certificate check is active and that the certificate is the authorized certificate
3. Confirm database hash

e. *PCS (Premier Central Scan) Scanner/PCs*

1. Ensure workstations are hardened to maximum extent possible consistent with Software.
2. Confirm program certificate check is active and that the certificate is the authorized certificate

f. *Adjudication Workstation*

1. Ensure workstations are hardened to maximum extent possible consistent with Software
  2. Confirm program certificate check is active and that the certificate is the authorized certificate
- g. *AccuVote TSx (Accessible Voting Unit or AVU for short)*
1. Install new version of BallotStation on the 200 units that are owned Repeat the Acceptance Test Done during original AVU acquisition
  2. Review AVU security including a hash code check of programs on data card
  3. Test new sip and puff and accessibility paddles for proper functionality
- h. Ballots to be printed for testing: 1,200 ballots from Contract's famous names test database (11 inch ballots on new test paper stock)
- i. **Acceptance Criteria/Measures of Success for Delivery Acceptance are:**
- i. All hardware and Software components were delivered, installed and are available for testing according to Contract terms.
  - ii. All models and model numbers match the Contract and other Documentation.
  - iii. The Software versions are those that have been certified at the federal and state level, if available, and agreed to by the County and the Contract.
  - iv. No hardware components are damaged.
  - v. No Software components are corrupted.
- j. Pursuant to state law any model or version numbers not matching the federally certified System, if available, will not be Accepted. Any damaged hardware components will be repaired or replaced by the Contract and any corrupted Software will be replaced by the Contract. Before beginning the next Acceptance Testing Phase, the Delivery Acceptance testing of each hardware and Software component shall be completed.

### III. **Mock Election Acceptance Testing**

- a. Build a mock election 15,000 18 inch ballots beginning with importing data from EMVR System and test each phase necessary for administering an election through results reporting. The mock election will include the following framework:
  - i. Data from the DIMS Election Management and Voter Registration System from a past election will be uploaded into server with a new version of GEMS
  - ii. Ballot Building and Layout
    1. Paper
      - a. Poll – English and Chinese
      - b. Absentee – English and Chinese
      - c. Provisional – English and Chinese
    2. Electronic – English and Chinese

- a. Audio – English and Chinese
- iii. Ballot Printing
  - 1. Creation of PRN files.
  - 2. Ballot on Request - print 200 ballots for voting test
  - 3. Data transfer to the ballot printer for printing test ballots (15,000) and Logic and Accuracy test ballots
- iv. Export card data into GEMS and import card data into DIMS
- v. Memory card creation
- vi. Ballots will be marked up with election contest selections by Contracts, staff (not involved in the testing process) and invited political party observers. Individuals not involved in the testing process will develop expected results.
- vii. Logic and Accuracy test with invitations to the political party observers and the Washington Office of the Secretary of State
- viii. Pre-scanning of ballots
- ix. Adjudication of ballots with a significant number of over votes, under votes, stray marks, and other anomalies normally seen on ballots returned by voters.
- x. Preparation of votes cast reports during the day (pre-election reports)
- xi. Use of AccuVote TSx (Accessible Voting Units) by two person groups following a voting script – both staff and party observers
- xii. Tabulation of the pre-scanned ballots
- xiii. Load the AccuVote TSx data cards into GEMS
- xiv. Confirm that tabulation results are accurate with party observer sign off to close the mock election
- xv. Report creation for election night
- xvi. Report creation for certification of the election
- xvii. Manual audit of Voter Verified Paper Audit Trail
- xviii. During the process stage a power outage to test UPS sufficiency and determine run time available on current battery setup
- b. As part of the Acceptance Testing the following data will be captured
  - i. Capture production rates on new Hardware. This will be necessary in determining how County staffing levels will need to adjust with the implementation of the new equipment
  - ii. Capture elapsed time for “final processing” necessary to produce the returns of votes cast reports on Election Evening. This final processing involves the counting (or tallying) of all pre-processed – pre-scanned ballots. Currently the County releases election results of votes cast on Election Night at 8:15 PM, the “final processing” time involved will need to be fully understood and Documented to facilitate the 8:15 PM public data release.
- c. **Acceptance Criteria/Measures of Success for the mock election are:**
  - i. All hardware and Software components required in order to conduct an election in King County function as Documented by the Contract, both individually and in concert with all other existing and

new hardware and Software components, in a real election environment simulating a Primary Election, from the beginning of the elections process to final tally, accounting and certification.

- ii. If a hardware or Software components do not function as required by federal and state law or as Documented by the Contract and the issue can not be resolved, or a System wide failure requires the restart of the mock election, then the System shall not be Accepted pursuant to the contract. The next phase of Acceptance Testing shall not commence until each phase of the mock election has been Accepted.
- iii. Acceptance of Hardware, Software and System does not occur unless each of the required tasks and functions listed above can be completed in a mock election environment.

#### **IV. Volume/Stress Acceptance Testing**

- a. To demonstrate the application architecture can perform acceptably at demand levels beyond normal values, using a significant number of ballots run through the System with a higher than anticipated number of ballots that would require electronic duplication.
  - i. 1.5 million previously folded ballots
  - ii. 300,000 ballots printed 14 inch
    - 1. ballots to be a primary ballot with preference races
    - 2. ballot built in English, Chinese and Korean
  - iii. 100,000 AVU ballots
  - iv. 30,000 ballots with write-in
  - v. 15,000 ballots with over votes
  - vi. 500,000 ballots with under votes
  - vii. 200 totally blank ballots
- b. As part of the test the following data will be captured
  - i. Capture production rates on new Hardware. This will be necessary in determining how staffing levels will need to adjust
  - ii. Capture elapsed time for “final processing” necessary to produce the returns of votes cast reports on Election Evening. This final processing involves the counting (or tallying) of all pre-processed – pre-scanned ballots. Currently the County releases election results of votes cast on Election Night at 8:15 PM, the “final processing” time involved will need to be fully understood and Documented to facilitate the 8:15 PM public data release.
- c. **Criteria/Measures of Success for the volume/stress test are:**
  - i. The equivalent of 1.5 million previously folded ballots can be scanned, processed and tallied in a time frame that allows for the tabulation of ballots as they are available for processing, so that certification deadlines can be met, public expectations met and without failure of the Hardware or Software or extraordinary human intervention.
  - ii. The System processes ballots printed by the primary print contractor.

- iii. The System imports, processes and counts 100,000 additional ballots from Accessible Voting Units (AVU) to ensure integration through the range of tabulation methods
- iv. The System processes the following volume of ballots in each category:
  - 1. 30,000 (2% of total) ballots with write-in votes; 15,000 (1% of total) ballots with overvotes; 300,000 (33.3% of total) ballots with undervotes; 200 totally blank ballots.
  - 2. The System must be capable of handling this volume of ballots to be acceptable pursuant to the Contract.

**V. Security Review Acceptance Test**

- a. The objective of the security review Acceptance Test is to identify security threats and vulnerabilities and to develop and Document mitigation strategies to maintain public trust and confidence in the voting System.
- b. Components of Threat Assessment – to be conducted by third party experts in computer security and elections professional(s) experienced in the administration of elections:
  - i. Reviewing the Independent Testing Authority reports from federal certification process as a starting point for the threat assessment. Identify areas not covered by the federal process and review/test those areas.
  - ii. With understanding that the California Top To Bottom Review was done on an older version of the product suite (not Assure version 1.2); review the new suite and Documentation to determine if issues identified in the California Top To Bottom Review with the TSx and GEMs Hardware and Systems have been mitigated in the new version of the solution suite (Assure 1.2) and if not, if the County's procedures sufficiently protect against remaining vulnerabilities.
  - iii. Review the report "Software Review and Security Analysis of the Diebold Voting machine Software" done for the Florida Department of State and examine if any of the flaws documented in the report have been mitigated by the newer version of the TSx Software and if not, if the County's procedures sufficiently protect against remaining vulnerabilities.
  - iv. Employ voting System threat modeling by examining the inputs and outputs of the System to assist in determining the structure of the intrusion/penetration testing.
  - v. Intrusion or penetration testing of the ballot tabulation System
  - vi. The third party security reviewers will conduct intrusion or penetration testing, of the functions and performance of the Premier Elections Solution Assure 1.2 voting System, to identify and document vulnerabilities, if any, to tampering or Error that could cause incorrect recording, tabulation, tallying or reporting of votes or that could alter critical election data such as election definition or System audit data.

- vii. The following specific security features or potential vulnerabilities of the of the System will be evaluated:
1. Is the encryption of the database implemented in a secure way and in such a way as to make meaningful manipulation of the database impossible?
  2. Can the database be accessed outside of the GEMS or PCS System?
  3. Are the program certificates of authentication implemented such that the certificates can be trusted to ensure application programs in use are the original unmodified federally certified applications, if available?
  4. Can the results from a ballot that was electronically duplicated be manipulated outside of the PCS application?
  5. Is it possible to preview cumulated election results within or outside the System going around established procedures and if all security features (including smart card technology) are properly implemented?
  6. Is the database replication among scanner units performed in a secure manner?
  7. Is application level access control performed by the security module adequate – can rights, privileges, use of smart card etc. be bypassed or escalated outside of the application?
  8. Are the scanned ballot images stored securely? Is it possible to access ballot images by bypassing any security controls?
- c. Collaboration with Elections Administration Expert(s) – consistent with the intent of the council it is required that the threat assessment include an election administration expert(s) to ensure that testing occurs in real world election environment and to assist with identifying policies and procedures to be used as mitigation strategies.
- d. **Acceptance Criteria/Measures of Success for the Security Review**
- Acceptance Testing**
- e. The System will be deemed Acceptable if:
- i. Any security vulnerabilities identified by information technology security experts can be mitigated by implementation of administrative policies, procedures and processes; are detectable through normally employed procedures; or are of a magnitude deemed to be highly improbable or of insignificant consequences.
  - ii. Warning notifications through printable documentation like audit logs are available and effective to alert election administrators of any attempt at unauthorized access or intrusion into the System.

In the event a probable or significant security vulnerability is identified that can not be mitigated through administrative policies, procedures or processes or a warning notification is not available to detect an identified attack the System shall not be Accepted.