Tips for a Secure Election

May 12, 2006

Election Systems and Software, Inc.
Corporate Headquarters
11208 John Galt Blvd.
Omaha, Nebraska 68137
United States of America
Phone: (402) 593-0101
Toll Free Inside of U.S.: (877) 377-8683
Fax: (402) 593-8107
http://www.essvote.com

Revisions for version 1.0, ES&S, Omaha, NE

Disclaimer

Election Systems & Software does not extend any warranties by this document. All product information and material disclosure contained in this document is furnished subject to the terms and conditions of a purchase or lease agreement. The only warranties made by Election Systems & Software are contained in such agreements. Users should ensure that the use of this equipment complies with all legal or other obligations of their governmental jurisdictions.

Intended Use:

Unity is an all–inclusive software system intended for a broad range of users and multiple equipment configurations. Each user is expected to be aware of their jurisdiction’s election equipment/system configuration and any specific election requirements, as well as their state and local laws and practices. Based on this awareness, each user must determine the Unity software features and options to be selected, and the process in which such configuration options are set or enabled.

Unintended and potentially adverse conditions or consequences could result if the Unity software and tabulation systems are not used appropriately. Some of these consequences include, but are not limited to, the following:

- Inefficient and/or non-productive time may be spent in the coding, configuration, and ballot layout processes.
- Configuration options may be set that are invalid for a jurisdiction’s election configuration and state or local laws and practices.
- Configuration options may be set that create invalid format and presentation of the ballot to the voter.
- Configuration options may be set that result in invalid, illegal, disabled, modified and/or unintended operation and/or process flows of the election system.
- Configuration options could be set that may provide confusing, undesirable, incorrect, or omitted election results tabulation and reporting.

Consult the Unity system documentation and your ES&S customer representative if you have any questions about the proper use of the Unity system.

Table of Contents

Chapter 1: Introduction

This checklist provides suggestions to help ensure the security of your elections. Always follow the processes and laws for your jurisdiction.

- □ No one individual should control all election procedures. The election supervisor should systematically assign responsibilities to many individuals in order to cover all phases of the election process.
- □ Formulate access control policies based on industry best practices and the jurisdiction's unique requirements.
- □ Perform background checks on all key election personnel.
- □ Log and report any, and all, security incidents.

The ES&S user guides and operator's manuals provide information about ES&S software and hardware.

Password Security

- □ The Election Administrator should control application password management.
- □ The System Administrator should manage Windows® PC password management.
- □ Use Audit Manager to assign passwords for Election Data Manager and ES&S Image Manager. Assign each user a unique password for Unity software.
- □ Do not share user names or passwords.
- □ Do not write down passwords.
- □ Change user names and passwords frequently for both Unity software and for your tabulators. At a minimum, change passwords for each election.

Physical Security

- □ **Election Security Best Practice:** Do not use PCs used for elections for any other purpose.
- □ Physically protect all computer systems that contain ballot definitions, telecommunications, or reporting software from access by unauthorized persons. The room where these systems are installed should be locked when the computer is unattended.

□ Maintain a secure warehouse setting, with controlled access to only authorized personnel, to store voting devices and/or tabulators.

Windows® Application

□ Run election systems only in their certified configuration.

□ Activate Windows® password controls for any computer used to run election generation or election reporting software.

□ Keep the election system as separate entity. The system on which you run your Unity software should only be used to run your Unity system.

Networks

□ Use virus protection on all computers running election programs that are connected to a network.

□ You can supply your network additional protection by using two LAN cards in the TCP Host system. Connect the cable from the router to the IP network to one card, and the office's LAN connection the other card. There is no way traffic from one connection can jump to the other.

□ Evaluate election systems and IT security program, policies, and applicable regulatory requirements. Perform a penetration test of systems in the election systems facility. Address any vulnerabilities identified during the assessment, with solutions for any infrastructure flaws, methods for closing security holes, and a determination of the policy framework required to support the information security function.

□ Use firewall protection for any computers running election programs that are connected to a network.

Tabulators

□ Keep track of keys.

□ Store these systems in a locked room when they are not in use.

□ Protect all terminals, PEBs, compact flash cards, and any other sensitive election supplies with the same degree of security as you use for paper ballots. Their security is essential to voter confidence.

Ballots

□ Track every election ballot, whether paper or electronic, throughout the entire election process.

Chapter 2: Election Set-up Security

Unity® Software

□ Only the System Administrator should be able to install and modify programs on the system.

□ Make a back-up file of the election definition, including ballot layouts, tabulator and voting machine coding, and audit logs of the setup, immediately prior to beginning the election creation process.

□ Restrict access to the folders containing the election database files with a password-protected login, if election-reporting files are stored on a network.

□ Reset passwords immediately after initially installing the product and for each following election period.

□ As soon as you finish creating an election, make a back-up file of the election definition, including ballot layouts and tabulator and voting machine coding.

□ To provide accountability, use formal signoffs in the verification stage of election file generation.

Audit Manager

ES&S recommends that you always use Audit Manager. The audit manager log function and user administration feature provide security for your election.

□ Print audit reports for every election and archive them physically and electronically with your other election materials.

Election Data Manager (EDM)

□ The EDM report function provides security for your election. Print reports for every election and archive them physically and electronically with your other election materials.

□ For iVotronic® voting systems, create an override password that must be used to keep the polls open after the specified closing time.

□ Use EDM reports as controls in the ballot proofing process.

Image Manager

- □ Use Image Manager .pdf ballot files as controls in the ballot proofing process.
- □ The iVotronic Image Manager (iVIM) audio report provides a written record of your audio ballot and security for your election. Print the audio report, and archive it physically and electronically with your other election materials.

Hardware Programming Manager (HPM)

- □ The HPM software provides a separate user security module that requires an administrator password and allows a maximum of 50 users.
- □ Use HPM reports as controls in the systems data/tabulator files creation processes.

Data Acquisition Manager (DAM)

- □ The TCP Host requires you to enter an election central password before processing results from remote counting sites.
- □ The DAM program setup password is highly recommended. Passwords to individual DAM program modules may be assigned to prevent users from changing the program settings for that module.
- □ Use a program access password for your host system. This password prevents unauthorized people from starting the Host before the polls close. It also prevents a person from stopping the program while data is coming in after the polls close.
- □ ES&S recommends that you assign passwords to all DAM programs and setup windows.
- □ ES&S recommends that you configure DAM to encrypt election results to add an additional layer of security to your reporting network.
- □ Use Modem Manager password options to limit user access to your network connections. Configure Acquisition Manager to encrypt polling place data to increase data transmission security.
- □ Modem Manager requires you to enter the program password before allowing data transfers from remote sites.
- □ Restrict the phone number for modems to authorized personnel only.
- □ If you use data transmission, use a different phone number for each election.

Election Reporting Manager

- □ Only install reporting software on the computer systems that you will use on election night.
- □ Lock up any additional computers that contain reporting software until the canvass is complete to prevent counterfeit reporting.

Chapter 3: Security While Preparing for Election Day

- □ Election personnel should receive the training and guidance necessary to minimize errors or misunderstandings.
- □ Election office volunteers and employees should maintain a spirit of professional integrity and carry out assigned duties in a manner that reflects the importance of the election process.
- □ Recruit poll workers and election judges by equal distribution among the various political parties.
- □ The election administrator should request that members of more than one political party serve as election judges at precincts, if it is not required by state law.

Location

- □ Arrange voting booths with the following considerations: traffic flow, voter privacy, and safety.

Paper Ballots

You are responsible for administrative control over the distribution and transport of all equipment.

- □ Use only coded ES&S specific ballot stock, with the specifications of the election definition. Other ballots will not be accepted by the scanners.
- □ Ensure that ballots are printed well before the election. Review ballots and make necessary corrections immediately after receiving ballot proofs.
- □ If multiple ballot print runs are required, follow the same procedures for proofing that were performed on the first printing. Make sure any additional ballot prints match the originals.
- □ Proof the content of all issues on the ballot before and after ballots are printed. Verify that all contest and candidates are present. Proof all issues and amendments for accuracy. Verify that each style contains correct lists of contest and amendments with candidates being in the correct order if candidates rotate, verify that ballot styles exist for each precinct and split as required for the elections.
- □ Prevent unauthorized access to official election ballots.

- □ Store ballots in a locked room or container between the point that ballots are delivered and Election Day.
- □ Record the number of ballots distributed to each polling location before they leave the election office. When ballots arrive at a polling location, poll workers should count the ballots again and compare the number of ballots delivered with the number counted at the election office. If the number of ballots delivered to the polling place and the number counted at the central site do not match, the poll worker should contact the election administrator immediately. Poll workers should record all ballot deliveries and quantities in the poll book.
- □ When the ballots are delivered to the polling place, proof the ballots to make sure the correct ballots were delivered to the correct polling place. Review the ballots to make sure all of the contests and candidates are present. Proof all issues and amendments for accuracy.
- □ Use a security escort when distributing ballots to each polling location.

Equipment

- □ Secure units in each location to the specifications of the county election officials. Examples of secure locations include locked rooms, closets, or offices.
- □ Testing your election prior to Election Day provides security for the election process. ES&S recommends that you always generate test decks and reports to test your scanners and reporting software for accuracy before the election.

  Election officials should perform a dry run test with election software and hardware that simulates, as closely as possible, specific conditions that may occur on Election Day and election night. Perform sufficient pre-election testing to ensure that any discrepancies between programming and the ballots can be identified.
- □ Create a ballot test deck to test all candidate and write-in positions.

  Configure the test deck to test the “vote for” allowance for each contest, under vote and over vote tallying and blank ballot tolerance. The ballot test should be easily verifiable by reviewing the report from the tabulator or reporting system.
- □ Test the ballots and system software/firmware before the election. Ensure that the results from the ballot tabulation equipment match the predicted results from the test ballots. Load test results into the reporting software, if applicable, and ensure that the results on the reports match the totals from the tabulation hardware. Perform all tests on the same system that will be used on election night.

- ☐ Store programmed memory cards securely at all times with logged accesses and transfers.
- ☐ Use controlled serialized seals that are tamper resistant and resistant to inadvertent breakage along with verifiable seal logs.
- ☐ Be sure the public count is set to zero before any new election activity.
- ☐ Be sure the terminal or scanner has passed the “clear and test” function.

Transportation

- ☐ Only election officials or their designees should transport DRE or optical scan precinct units. Upon delivery, election officials or their designees will obtain sign off of which units were delivered to each specified location. The delivery list will be provided to the election officials at the count to ensure that the proper units were delivered to the correct locations.

iVotronic® Voting System

- ☐ Immediately after the compact flash card is installed in the voting station, seal the card against unauthorized access.
- ☐ Place seals on the iVotronic voting booth and communications pack to prevent opening the unit, which could grant access to voter terminals and PEBs without detection.
- ☐ Seal PEBs programmed for the election in the communication pack using a tamper-evident, numbered seal that is written down and maintained by an election official. Provide the seal numbers of the units to the poll worker who will verify the seal numbers before breaking the seals on Election Day.
- ☐ Secure the top and bottom of booth covers using numbered seals. Write down the seal numbers and maintain a record of the numbers. Provide the seal numbers of the units to the poll worker who will verify the seal numbers before breaking the seals on Election Day.
- ☐ Do not set the voting station into election mode until after the compact flash card is sealed inside.
- ☐ **Election Best Practice:** The election coding center programs a specific number of supervisor PEBs with ballots. Election headquarters distributes these PEBs to precinct officials separately from the voter terminals. These procedures place election security in the hands of the precinct officials, rather than taking security measures at the equipment storage facility.

- □ Precinct officials must open terminals with the password before tabulation begins. This places election security in the hands of the trained precinct officials instead of solely on the equipment storage facility.

iVotronic*LS*® Voting System

- □ Place numbered seals on terminals to prevent unauthorized users from opening the unit and gaining access to the terminal without detection.
- □ Secure programmed EBAs in the same manner as printed ballots.
- □ Use separation techniques to prevent tampering of any hardware used in an election. In order to load data, an operator must be in possession of a properly qualified EBA and an external password communicated by election officials. (This means that in order to manipulate votes, someone must possess the password, the EBA that was used on an LS terminal and a complete, LS terminal in order to gain unlawful access.) Proper election security procedures can preclude this possibility. In addition, the iVotronic*LS* design requires that administrators follow the election process in the proper sequence. Any functions that do not follow the proper sequence, such as closing the polls before the legal closing time, require an election–specific password that should be secured and communicated only on an exception basis through proper election procedures. In sum, the iVotronic*LS* design provides tamper proof hardware that can only be operated in the proper election sequence.
- □ Precinct officials must open terminals with the key-activated supervisor switch before tabulation begins. This places election security in the hands of the trained precinct officials instead of solely on the equipment storage facility.

All Optical Scanners

- □ Clear and test each machine. Set scanner totals to zero.
- □ Do not use a terminal or card that already contains votes.

Precinct Scanner

- □ Secure the PCMCIA card in the scanner using a numbered seal after the election coding and the units are pre-tested. Election officials should write down the number on the seal. When units are delivered to the polling locations, poll workers will verify that the number of the seal is the same as was written down by the election officials preparing the units for the election.

- □ Secure the scanner with a security shield to cover the PCMCIA card. Lock the M100 to the top of the ballot box, to prevent the security shield from tampering.
- □ Precinct officials must open scanners with the key-activated supervisor switch before tabulation begins. This places election security in the hands of the trained precinct officials instead of solely on the equipment storage facility.

Central Count Scanners

- □ Plan the route and location of the ballot storage area before Election Day. The clerk should appoint people to be responsible for removing all scanned ballots from the scanner output hopper and returning them to the ballot box. These people should then remove the box containing counted ballots from the work area, and place it in the designated storage area.
- □ Secure central count scanners in a locked room within the county.
- □ Secure the disks used for programming at the county site until used for processing on election day.
- □ Make sure the back door of the scanner is closed and locked.

Chapter 4: Security During Election Day

- □ Make sure the public count reads zero before opening the terminal for voting.
- □ Reconcile ballot quantities at the precinct level.
- □ Secure the entrance to the polling place.
- □ Validate all poll watchers and maintain a list of what each watcher can and cannot do. Make this list available to your poll workers. A poll watcher is an individual who represents a candidate, political party, independent organization or a proponent or opponent of a referendum who is legally inside the polling place to observe the conduct of the election. This can include precinct captains, political workers, and supporters of a candidate or members of an organization. A number should also be available to the poll workers to call if the polling place becomes overcrowded with poll watchers.
- □ Verify each voter’s identity according to local laws and practices.
- □ Periodically, check terminal vote counts against poll book-based tallies and the records of spoiled ballots.
- □ When results are transmitted or physically transported to a central site for tabulation and reporting, balanced controls between precinct tapes and central reports should be used as processing controls.

All hardware

- □ Be sure that the ballot box doors that allow access to the ballot bins are locked.
- □ Lock the ballot entry door on the ballot box when the scanner is not mounted on the ballot box. Make sure the door is open before mounting the scanner. If the door is not open when the scanner is mounted, ballots will jam.
- □ Lock the Emergency Ballot Bin on the ballot box with the door closed.
- □ In the unlikely event that the scanner becomes inoperable, unlock the emergency ballot bin, open the ballot slot, and then relock the emergency ballot bin.
- □ During tabulation, monitor system use to ensure that no unauthorized personnel tamper with the equipment.
- □ Close the M100 before attempting to print results tape that shows vote totals for all candidates and questions.

iVotronic® Voting System

□ Do not distribute PEBs prior to election day.

□ Use only opaque bags or envelopes to transport PEBs.

□ Release PEBs only to know, trusted personnel.

□ When distributing PEBs, use tamper-evident, numbered seals on all PEB carriers.

□ Have at least two poll workers, preferably from different political parties, check the integrity of the seals and witness the breaking of the seal on the PEB carrier in the polling place.

□ Cross check each terminal's protective count against the public count.

□ Election officials should not provide precinct officials with the menu passwords, other than the main menu. If precincts require the service menu or election central application menu passwords, extenuating circumstances exist and trained support personnel should be present at that precinct to oversee the situation. During voting, a poll official should only access a terminal's administration menu if instructed to do so by the jurisdiction's election administrator.

□ If you use voter-activated terminals, inspect each PEB after it is returned from activating a ballot to ensure that the serial number on the PEB matches the number logged when it was given to the voter.

□ Only use the supervisor PEB to open and close terminals, and lock it in a secure location at all other times.

□ Never leave the supervisor PEB unattended or use the device for any purpose other than opening voting terminals at the designated poll opening time, closing the terminals at the end of the day or resolving a special condition that requires an operator to access a terminal's administration menu.

□ Monitor all PEBs to ensure that they are never removed from the polling location.

□ Secure the entire roll of RTAL printer paper into a secure envelope that is designed so that the inside contents are not visible. Seal the envelopes with labels noting the election date, county, and polling location. Follow this procedure both when replacing a paper roll during election day, and as part of the closing process, if you are allowed to replace paper.

□ Verify public count against the number of voters recorded in the poll book throughout the day.

□ Voter terminals do not allow voting until the terminal is properly opened by the Supervisor PEB.

- □ Investigate all audio alarms to ensure the voting device has not been tampered with and is functioning correctly.
- □ Ensure that you close all terminals.

iVotronic*LS*® Voting System

- □ A poll worker must use the appropriate EBA and password codes to open an LS terminal before a voter can cast a ballot.
- □ Verify the election EBA is for the correct polling place when opening the polls.
- □ Cross check the public count against the number of voters recorded in the poll book and crosscheck the protective count for each terminal against the terminal's public count.
- □ Election officials should not give menu passwords to precinct officials. If precincts require the Service Menu or Election Central Application Menu passwords, extenuating circumstances exist and trained support personnel should be present at that precinct to oversee the situation.
- □ Issue only one election EBA to a precinct.
- □ Make sure the public count reads zero before opening terminals for voting.
- □ Only allow election officials to handle EBAs.
- □ Poll workers must know the election password in order to be able to use the election EBA.
- □ Poll worker must select the correct ballot from the poll worker panel if you have multiple ballots.
- □ Poll workers must enter an override password to close polls early or to allow voting after the official poll closing time.
- □ Precinct officials must maintain constant possession of the election EBA.
- □ Voter terminals must be zero to open. If a terminal that contains votes is deactivated in an open state (such as an unforeseen power loss) the poll worker must insert a proper EBA and enter the override password for the election and password before resuming the voting session.

Paper Ballots

- □ At the polling place, maintain a ballot accounting record to track ballots received from the election office, a count of ballots completed by voters, and defective ballot count, and the count of all unused ballots after the polls are closed. Defective ballots are ballots that are misprinted, damaged, or returned for replacement due to mistakes made by the voter. Reconcile all ballots received with those used (voted or spoiled or defective) and leftover for each ballot style.
- □ Be wary of paper ballots that contain suspicious candidate markings. Ballots that appear to be automatically marked by a computer printer or typesetting equipment indicates an attempt to introduce fraudulent ballots into the election process. Similarly, response areas marked with stickers or straight-line pencil strokes that overstrike the response target might also indicate fraud.
- □ Place all ballots, unvoted, spoiled, defective, into a lockable storage container with a copy of the printed precinct tape if using a precinct system, and ballot accounting record. Transport to the central tabulation center.
- □ Prior to tabulation, assign security personnel to escort ballots from the receiving area to the tabulation area. During tabulation, carefully route paper ballots through the tabulation area in order to prevent skipped or redundant counts. After tabulation, move all ballots to a locked storage area to prevent unauthorized access.
- □ When ballots are received at the tabulation center, the ballot accounting record should be examined and the ballot reconciliation verified. If you use a precinct tabulator, verify the vote counts on the enclosed results tape with values from the results media. All voted ballots should be returned to a locked container, along with any unvoted or defective ballots. Store the ballot containers in a locked room until tabulation begins. Secure all unmarked ballots as well, to prevent fraudulent marking.

Chapter 5: Security After the Polls Close

Reporting requirements may vary according to state laws. Develop a plan for organizing and managing the reporting process during the election. Make sure that the necessary reporting is performed at the end of the process.

- □ The election administrator should request that responsibilities for receiving ballot boxes and scanning ballots be separated.
- □ Inspect paper ballots for automated marking when they arrive at the counting location.
- □ Examine the audit log attached to your tabulator's log printer and, if applicable, the audit reports generated by your reporting software. Inspect the reports for correct procedures and errors.
- □ Make backups of all tabulation reporting electronic files, including results database and audit logs.
- □ Print final reports, examine the results, place all documentation in a sealed envelope and lock the documents away for canvassing.
- □ Save all reports generated by the election tabulation equipment as well as the reports generated with reporting software. Collect and save all audit reports and store them with final reports.
- □ Unless required by law to save interim reports, destroy all interim reports after the counts are disseminated to the public to prevent the accidental introduction of these reports as "current" counts later in the evening.
- □ Store all back-up files and scanner disks with results in a locked room designated for election material storage.

Location

- □ Maintain a secure tabulation center with controlled access to only authorized personnel.
- □ Use personnel badges to identify authorized personnel.
- □ Maintain a high awareness of security, which can include but not be limited to the following.
  - Visible security personnel
  - Frequent badge checks.
  - Occasional "perimeter penetration" checks using unauthorized personnel to maintain employee vigilance.

- □ Establish a clear traffic route for election materials received from polling places (ballot boxes, memory cards, etc.) and a route from tabulation equipment to the ballot storage location. This route should be clearly marked as “restricted,” and only authorized personnel should be in the areas where election results are transported. Authorized personnel should be identified with official badges or cards. Restrict access to the tabulation and ballot storage areas to authorized personnel only. These areas should be locked when not in use. To avoid confusion, establish the tabulation and ballot storage areas in separate locations.

All hardware

- □ In post-election mode, print the results report prior to removing the memory card from an optical scanner. If additional reports other than the results report are available, print these as well.
- □ Remove election definition media from the equipment and store it in a separate, secure area when the tabulators are not in use.
- □ If precinct tabulators are to remain on site after the polls close, county election officials determine with the location officials the best secure location for the units until the units can be picked up by election officials or their designees.
- □ The back door of central count scanners should be closed and locked.

Audit Manager

- □ Archive/export audit logs from Audit Manager and reset it to blank immediately after all of the tasks for an election are complete. Keep audit archives with all archive materials for that specific election.
- □ Examine the audit log attached to your tabulator’s log printer and, if applicable, the audit reports generated by your reporting software. Inspect the reports for correct procedures and errors.

iVotronic® Voting System

- □ After totals have been obtained when the polls are closed, remove the PEBS, secure the iVotronic with numbered seals. Return the PEBs used for the election to the communication pack and seal with numbered seals. Write down the seal numbers and provide the numbers to the election officials with the election results.

□ Prior to tabulation, assign security personnel to escort electronic ballots and PEBs from the receiving area to the tabulation area. During tabulation, carefully route PEBs through the tabulation area in order to prevent skipped or redundant counts. After tabulation, move all PEBs and electronic ballots to a locked storage area to prevent unauthorized access.

Election Reporting Manager (ERM)

□ Balance and validate vote counts as a control mechanism between ERM reports generated at a central count location and results reports generated by precinct tabulators.

□ Cross-verify results by comparing the total votes for each contest (candidate votes + over votes+ under votes) to the number of ballots that were eligible to vote in the contest.

□ The Election Administrator must collect and archive the audit and event logs and back them up on permanent storage media.

Chapter 6: After the Election

- □ Retain all of the physical ballots cast in an election as a redundant means of verifying or auditing election results.
- □ Store all paper ballots from the election in a locked room designated for election material and ballot storage.
- □ Store all systems in a locked room when they are not in use.
- □ Make a backup file of your election immediately following election certification/ canvassing.
- □ Clear the election before you start the next election.

Index