



Secretary of State
DEBRA BOWEN
State of California

March 17, 2008

Steve Pearson
Vice President, Certification
Election Systems & Software
11208 John Galt Blvd.
Omaha, NE 68137

Fax: (402) 970-1276
smpearson@essvote.com

BY FAX, EMAIL AND POSTAL MAIL

Re: Application for California Certification of Unity version 3.0.1.1/AutoMARK Voting System

Dear Mr. Pearson:

As you know, on February 15, 2008, the final reports on state certification testing of the Unity version 3.0.1.1/AutoMARK Voting System were provided to Election Systems & Software ("ES&S") and the public. At a public hearing held in Sacramento on February 20, 2008, the consultants responsible for testing the system reported their findings, and ES&S and members of the public were given an opportunity to present their views on the testing reports and the voting system.

I have reviewed the testing reports and the proposed California Use Procedures for the voting system submitted by ES&S, which I received on March 4, 2008. Based on that review, I am denying the application for certification at this time for the reasons set forth below. ES&S may request reconsideration of the denial, but only if it does so within 45 days of the date of this letter and after it has complied with the two conditions set forth below.

The grounds for denial of the application is ES&S's continued failure to submit proposed California Use Procedures that satisfactorily address issues ES&S has known for months would almost certainly be required for certification. ES&S has had the details concerning those conditions since early December 2007, when I issued the conditional recertification of the very similar, predecessor version of this voting system, Unity version 2.4.3.1/AutoMARK. ES&S has also been aware that immediate effort was required to make the required Use Procedure revisions promptly for the conditional recertification of Unity version 2.4.3.1/AutoMARK to remain effective.

As ES&S and many local elections officials have correctly observed, the security of a voting system involves not only the hardware and software components of the system itself, but also the election administration procedures and training followed by elections officials and poll workers. Complete, up-to-date Use Procedures that address a voting system's known security issues are essential to ensuring those measures are effective. The reports from the functional testing, red team analysis and source code review of this voting system revealed multiple and extremely serious security vulnerabilities. (A summary of the report's findings is included here as Attachment A.) Approval for use cannot be considered absent clear, detailed California Use Procedures that require adherence to strict, mandatory physical and administrative security requirements. ES&S has not provided this critical piece of the overall security puzzle. Without it, I cannot certify the voting system for use in California.

In the letter to me dated January 11, 2008, from John Groh, Vice President of ES&S, Mr. Groh went point-by-point through the conditions set forth in the December 7, 2007, conditional recertification of version 2.4.3.1 of the system. (A copy of the letter is included here as Attachment B.) In at least eight instances, Mr. Groh stated that ES&S was working on and would provide revisions to the California Use Procedures to satisfy important conditions of the recertification. (See Attachment A, items 2, 4-Part I, 4-Part II, 8, 10, 11-Part B, 16 and 18.) For example, Mr. Groh's response on item 4 states:

Item 4 - Part II: Automated Configuration Verification Utility

SOS Condition: The vendor must identify automated mechanisms for jurisdictions to confirm and document that their system has been configured to these standards, and that all updatable components are the approved version and level. The vendor must provide full instructions for the use of these mechanisms, including expected results.

ES&S Response: ES&S is investigating a validation utility from the Center for Internet Security ("CIS") that would be used to check the configuration of the PC. ES&S will download and test this utility and upon approval from the Secretary of State, will work with the County Election Administrators to develop a procedure for its installation and use. In addition, ES&S has a utility that was developed for newer versions of the Unity Software that will report a file hash for each application file that can then be compared with the approved hashes published with the certification to verify that all appropriate files are present and unaltered. On successful completion of these tests and upon approval from the Secretary of State, ES&S will work with the County Election Administrators to develop a procedure for its installation and use following the February 5th election.

At the February 20, 2008, public hearing on the application for certification of the updated version of the system, Mr. Groh assured Deputy Secretary of State for Voting Systems Technology and Policy Lowell Finley that ES&S had completed the draft

Steve Pearson
March 17, 2008
Page 3

revised California Use Procedures, which was undergoing legal review and would be provided to my office within days. Mr. Groh also stated that ES&S would promptly respond to the findings in the certification testing reports for Unity version 3.0.1.1/AutoMARK issued on February 15, 2008, by making additional revisions.

ES&S submitted what it stated were its revised, completed California Use Procedures on March 4th. Staff spent several days reviewing the document, which is several hundred pages in length. Staff found revisions expressly called for in the testing reports, but found that none of the changes promised two months earlier in Mr. Groh's letter of January 11, 2008, were included.

Two months have passed since ES&S promised detailed Use Procedure revisions addressing problems in the security and auditability of their voting system. ES&S has fallen short in two respects. First, it has yet to address those problems in the revisions to the Use Procedures for the currently certified version of the system, Unity version 2.4.3.1/AutoMARK. As you know, this was an explicit condition of the December 2007 recertification. Second, ES&S has not addressed those same issues in the revisions to the Use Procedures for Unity version 3.0.1.1/AutoMARK. Under the circumstances, I cannot approve use of the Unity version 3.0.1.1/AutoMARK voting system at this time.

The application for certification of the Unity version 3.0.1.1/AutoMARK voting system is denied. ES&S will be permitted to apply for reconsideration of the denial within 45 days of the date of this letter if it first satisfies two conditions:

(1) On or before April 8, 2008, ES&S must submit complete revisions to the California Use Procedures for the Unity version 2.4.3.1/AutoMARK voting system that fully satisfy the conditions of the conditional recertification of the system dated December 7, 2007.

(2) On or before April 15, 2008, ES&S must submit complete revisions to the California Use Procedures for the Unity version 3.0.1.1/AutoMARK voting system that fully satisfy the conditions of recertification for Unity version 2.4.3.1/AutoMARK dated December 7, 2007, as well as the specific revisions recommended in the testing reports for Unity version 3.0.1.1/AutoMARK. (As previously stated, the draft received on March 4, 2008, complies with respect to the specific revisions recommended in the testing reports.)

Sincerely,



Debra Bowen
Secretary of State

DB:lf:elg

cc: Mr. John Groh, Vice President, ES&S

Mr. Sheldon Johnson, Clerk-Recorder, Amador County
Ms. Karen Varni, Clerk-Recorder, Calaveras County
Ms. Kathleen Moran, Clerk-Recorder, Colusa County
Mr. Stephen Weir, Clerk-Recorder-Registrar of Voters, Contra Costa County
Ms. Elaine Ginnold, Registrar of Voters, Marin County
Mr. M. Stephen Jones, Clerk/Registrar of Voters, Merced County
Ms. Jill LaVine, Registrar of Voters, Sacramento County
Ms. Julie Rodewald, Clerk-Recorder, San Luis Obispo County
Mr. Joseph Holland, Clerk-Recorder-Assessor, Santa Barbara County
Ms. Colleen Setzer, Clerk, Siskiyou County
Mr. Ira Rosenthal, Registrar of Voters, Solano County
Ms. Lee Lundrigan, Clerk-Recorder, Stanislaus County
Ms. Deborah Russell, Clerk/Auditor-Controller, Tuolumne County



Summary of Results from California Testing of the ES&S Unity 3.0.1.1/AutoMARK Voting System

The California Secretary of State tasked Freeman Craft McGregor Group (FCMG) to perform functional testing, accessibility testing, “red team” analysis (penetration testing) and source code review of the ES&S Unity 3.0.1.1 Voting System (“ES&S Voting System”). On February 15, 2008, FCMG provided public written reports on each area of testing and review, supplemented by private and confidential red team and source code review reports that went into greater depth on security-sensitive information. The major findings of the reports are summarized below.

Functional Testing

The report on the functional testing of the system concluded the system was capable of performing all necessary functions. The functional testing, however, also revealed many serious deficiencies in the security features of the system.

First, the testers noted that, as part of the California Use Procedures, instructions for securing the system are required. In the draft Use Procedure provided by ES&S for this testing, a copy of the Center for Internet Security’s (CIS) Windows XP Professional Operating System Specialized Security- Limited Functionality Benchmark Consensus Baseline Security Settings guideline was given as the recommended operating system “lock-down” setup to be applied to the Unity and AIMS workstation. Although that high level of “lock-down” of the operating system would be desirable in an election system, the actual use of the guideline recommended by CIS assumes careful testing by application developers or information security personnel to determine what portions of the checklist could safely be applied or adapted without denying the services and resources needed for the application to function. There was no evidence in the form of adjustments or instructions that ES&S had performed the necessary testing to apply the guideline at the level presented. As a result, the testers declined to setup the test environment to that level, and instead applied only basic elements of the Legacy level of the CIS checklist, terminating only services that were known to be vulnerable and recommended by the Microsoft Security Program office.

Second, the testers reported that ES&S largely depends on the basic Windows login accounts and physical and procedural security provided by the local client’s Information Systems staff or equivalent to protect the Unity operations. Application level user account passwords, where they are used, are similar in complexity to the default Windows login passwords, which is considered a weak password scheme.

Third, for the Hardware Programming Manager (HPM) (critical because it can be used to change the election definition) and Election Reporting Manager (ERM) (critical because it has the functionality to change votes in the reports) the only protection from malicious attacks is restricting physical access to the workstation.

Accessibility Testing

Accessibility testing was conducted by Noel Runyan of Personal Data Systems and Jim Tobias of Inclusive Technologies. Following a review that included expert “walk-throughs” of the system and testing by voters with a wide range of disabilities, their report concludes that the ES&S Unity 3.0.1.1 Voting System (with AutoMARK and M100 Scanner) is substantially compliant when assessed against the requirements of the Help America Vote Act (HAVA) and specified in the 2005 VVSG guidelines. The report concludes the system represents an adequately accessible voting system capable of effectively serving the large range of voters with disabilities that should be accommodated according to the HAVA requirements.

The accessibility report did note, however, several areas in which the accessibility of the AutoMARK ballot-marking device could be substantially improved. Improved ballot privacy sleeves and handling procedures are needed; the force required for ballot extraction is excessive; unnecessary ballot marking errors and high voter frustration are caused by the lack of confirmation dialogs before canceling or exiting the write-in function and before marking and returning the ballot; speech synthesis and audio interface controls could be improved; switching modes for the controls in the summary and verification reviews place heavy cognitive loads on audio-only voters; and more voters could make better use of the visual display if its magnification range and use of color was enhanced.

Red Team Analysis

The goal of the red team analysis (penetration testing) was to compromise the security of the voting system. The team demonstrated that several components of the voting system are vulnerable to attack.

PCMCIA cards used by M100 Tabulators may be exchanged at the precinct during an election to implement ballot box stuffing attacks in favor of particular candidates. This exploit is difficult to detect without examining the audit logs.

All data on the PCMCIA card used by M100 Tabulators is unencrypted and can be viewed using commonly available programs. This enables a potential attacker to analyze the data on the card and develop strategies to defeat the embedded security mechanisms.

An attacker with unauthorized access to the Election Reporting Manager (ERM) can modify election results. The Red Team identified an exploit that enables the unauthorized access. Upon gaining access to the ERM, the attacker can manually add or remove votes from the official vote totals. Note that the ability to manually edit vote totals is necessary to correct errors, but only authorized individuals should have access to this feature. The

attack would take a few seconds and, if executed properly, could only be detected by analyzing audit logs.

The Zip disk containing the M650 Tabulator results may be modified while it is transported to the Election Reporting Manager (ERM), which would process the modified vote totals without questioning their validity.

An attacker with unauthorized access can gain complete access to the Audit Manager database by cracking the password. Once access to the database is gained, attackers can change records, obtain, create or remove login credentials for the Audit Manager, Election Data Manager, or ES&S Image Manager (ESSIM) and delete audit log entries to cover their tracks.

An attacker with unauthorized access could modify stored procedures in the Microsoft SQL Server database used by the AutoMARK Information Management System (AIMS). The exploit gives the attacker the ability to write modified ballot definition files data to the Compact Flash cards used by all of a jurisdiction's Voter Assist Terminals. The attacker could modify the audio/visual information of the ballot so a voter using the audio ballot would hear the name of one candidate but the device would mark a vote for another candidate.

An attacker with unauthorized access working with a computer systems expert could disable the access control system for the Hardware Programming Manager (HPM) and the Election Reporting Manager (ERM) in a few minutes. As noted earlier, unauthorized access to the HPM and/or ERM constitutes a serious breach of voting system security. HPM can be used to change the election definition and ERM can be used to change results in the reports.

An attacker with unauthorized access could also tamper with the access control system for the Hardware Programming Manager (HPM) and the Election Reporting Manager (ERM) to selectively grant (or deny) any individual the right to access the HPM and ERM.

An attacker with physical access to the system and the appropriate expertise could obtain the password for accessing the Hardware Programming Manager (HPM) and Election Reporting Manager (ERM) in a few minutes.

An individual with sufficient expertise can pick the locks located in the front of the Voter Assist Terminal (VAT), the M100 Tabulator and the M650 Tabulator. The time taken by the red team to pick the VAT, the M100 and the M650 locks ranged from five seconds to one minute.

The wire seal on the front panel of an M100 Tabulator can be bypassed. The wire security seals tested by the red team were provided by ES&S. If a seal is not tightened correctly, an attacker can bypass the seal on the front access panel of the M100 providing a vector of attack on the PCMCIA cards.

The Voter Assist Terminal (VAT) and M650 Tabulator incorporate several paper seals whose damage or removal are designed to indicate tampering. The red team used commonly available products to cleanly remove the paper seals on the VAT and M650 back panel without damaging them or triggering the paper seal voiding mechanism.

Source Code Review

The review of the voting system's source code was performed by atsec Information Security Corporation. The reviewers concluded that users of the system should not rely on the claimed security measures. Their public report provides the following summary of results:

“The system is designed to execute code supplied on the election definition memory cards on the precinct ballot counters, with no effective measures to ensure integrity and authenticity of this code. Due to this, there is little assurance that the systems will actually be running the reviewed code at election time.

“The system fails to provide strong Identification and Authentication for access control. Some components have no access controls at all. For those components that do restrict access by requiring a User ID, a password, or a User ID/password pair, the login credentials are either hard coded in the source code, stored in clear text in a database, or at best, scrambled with extremely weak algorithms that do not prevent credentials from being discovered. Thus, all components in the system are potentially exposed to unauthorized access.

“The system fails to provide confidentiality and integrity of election data (including election definitions and election results). The election data is transferred among components of the Unity System via removable media devices. The data on the media devices is either in plain text, stored with simple checksum values, obfuscated with extremely weak homebrewed algorithms, or at best encrypted with symmetric algorithms. In cases where the data to be transferred is encrypted, the encryption keys are hard coded either as a plain ASCII string or with a simple obfuscation that can be easily reversed. The election data can be maliciously modified by a component of the Unity System or during the transition of the media from one component to the other, but yet still be treated as valid by other Unity System components.

“The system fails to provide reliable accountability for audit logs. Audit logs of the Unity system are kept either in databases or log files, none of which are protected by any kind of tamper-detection mechanism. The audit log of the system is susceptible to tampering without being detected.

“The developers generally assumed that input data will be supplied in the correct expected format. There is little validation checking of the data, leading to potentially exploitable vulnerabilities when those assumptions turn out to be incorrect, for example,

due to malicious manipulation of the election definition leading to execution of attacker supplied code.

“The security of the Unity System depends on its secure use, which assumes that all parties involved in developing, maintaining, distributing, deploying and using the Unity system must be trustworthy. This assumption is equivalent to saying that there are no threats to the Unity system.”



January 11, 2008

**VIA E-MAIL TRANSMISSION
AND OVERNIGHT DELIVERY**

Honorable Debra Bowen
Secretary of State, State of California
1500 11th Street, 6th Floor
Sacramento, CA 95814

**RE: Additional Conditions for Use of Election Systems and
Software, Inc. ("ES&S") Optical Scan Voting System**

Dear Secretary Bowen:

ES&S received your letter dated December 7, 2007 on Tuesday December 11, 2007, in which you introduced 39 conditions which must be met in order for California counties to continue to use ES&S's optical scan voting system 2.4.3 version.¹ A number of these conditions asked that ES&S present to you plans, specifications, and/or procedures within only 15 days, which was simply not possible. ES&S has now had a reasonable opportunity to carefully review the conditions specified in your letter and submits the following response to the conditions that arise out of or have been placed on the use of ES&S's optical scan voting system in the State of California.

Initially, ES&S wants you to know that it respects and concurs with your goal that voting systems be accurate and secure to the highest degree practicable. Alarming, these December 7 conditions were issued only 60 days before the February 5 Presidential Primary; they were substantial in scope; and their implementation had to be commenced during the holiday season, which effectively reduced the 60-day period. Respectfully, we are seriously concerned over the execution of many of the action points as such items may place an insurmountable burden on the California county Election Administrators involved and may, in fact, affect the integrity of the February 5, 2008 election.

¹ The current optical scan voting system is Unity version 2.4.3.1 as certified by the California Secretary of State on March 31, 2006, as set forth in the Secretary of State's approval letter of even date, attached hereto as Exhibit A.

However, while reserving our rights, our goal is to make every effort to complete those action items capable of completion before the election and to establish a realistic timetable and plan for completion of the remaining longer-term items for purposes of the June election. ES&S wants to cooperate with your office. Accordingly, ES&S has attached to this letter a point-by-point response (including our set of recommendations and the status of our efforts) with respect to each of the special use conditions that you set forth in your December 7, 2007 letter. In addition, ES&S has prepared and encloses (via overnight delivery) its latest draft of its Draft California Election Procedures ("Election Procedures") in response to a number of the conditions, as appropriately referenced within the enclosed responses. ES&S requests that you review each of the enclosed responses and the Election Procedures, as ES&S will be asking each California County Election Administrator to do the same.

Still, please be aware that full compliance with many of these points will require an additional time period, depending upon the nature and scope of the requested action item. Even this time frame assumes that all California jurisdictions will be able to provide ES&S with full resources to complete the applicable action items.

As referenced above, ES&S has prepared and is including the latest DRAFT of its California Election Procedures document. You will find this document as supplemental response to a number of conditions, as appropriately referenced within our submitted responses. Complimenting this Draft of our Election Procedures are four additional documents. The following documents are also being submitted to you via overnight delivery with a copy of the draft Election Procedures:

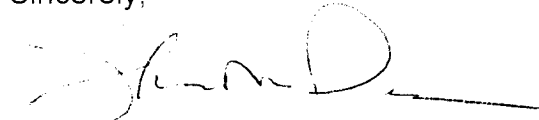
- California Election Procedures Manual for the ES&S Model 100 Scanner
- California Election Procedures Manual for ES&S Central Scanners (Models 550 and 650)
- California Election Procedures Manual for the ES&S AutoMARK Voter Assist Terminal
- ES&S' Tips for a Secure Election, dated May 12, 2006

All of these items are being reviewed and updated to include the most recent California Voting System Procedures. We will deliver the final version to your office as soon as it is completed.

Honorable Debra Bowen
January 11, 2008
Page 3

ES&S looks forward to your response and an expedited discussion of the enclosed responses with your Office, as well as continued efforts to support the California counties affected. We are prepared to meet with your staff immediately in order to coordinate and implement our responses. If you should have any questions or would like to schedule a time to meet to discuss our responses, please contact me directly.

Sincerely,



Steven M. Pearson

Enclosures

cc: Sheldon D. Johnson/George Allen, Registrar of Voters, Amador County
Karen Varni, County Clerk, Calaveras County
Kathleen Moran, County Clerk-Recorder, Colusa County
Stephen L. Weir, County Clerk, Contra Costa County
Elaine Ginnold/Melvin Briones, County Clerk/Registrar of Voters,
Marin County
M. Stephen Jones/Deanna Brown, County Clerk-Registrar,
Merced County
Jill LaVine, Registrar of Voters, Sacramento County
Julie Rodewald/Tommy Gong, County Clerk-Recorder,
San Luis Obispo County
Joseph E. Holland/Renee Bischoff, Clerk-Recorder-Assessor,
Santa Barbara County
Colleen Setzer, County Clerk, Siskiyou County
Ira Rosenthal, Registrar of Voters, Solano County
Lee Lundrigan, County Clerk-Recorder, Stanislaus County
Deborah Russell/Jackie St. George, County Clerk-Auditory-Controller,
Tuolumne County

EXHIBIT A



BRUCE McPHERSON | SECRETARY OF STATE | STATE OF CALIFORNIA

OFFICE OF VOTING SYSTEMS TECHNOLOGY ASSESSMENT

1000 STREET 85, SACRAMENTO, CALIFORNIA 95834 | TEL: (916) 227-2200 | WWW.SOS.CA.GOV

March 31, 2006

Steve M. Pearson
Election Systems & Software, Inc.
11208 John Galt Blvd.
Omaha, NE 68137

Dear Mr. Pearson:

We have received your request for approval of modifications to your currently certified Unity Software.

On December 9, 2005, the Secretary of State received an application for administrative certification of the existing certified system to incorporate a modification that resolves the problems encountered in reporting election results by Sacramento and Solano Counties.

ES&S currently has two voting systems certified in California that incorporate the Unity version 2.4.3 election management software which was first certified for use on October 27, 2004. The Unity software is a suite of sub-component applications composed of the following modules:

- Audit Manager v. 7.0.2.0
- EDM v. 7.2.1.0
- iSSIM v. 7.2.0.0
- IPM v. 5.0.3.0
- IRM v. 6.4.3.0

ES&S has modified the IRM module of the Unity application to address and correct the identified problem. The new, corrected version of IRM is 6.4.3.3, updating Unity to version 2.4.3.1. NASED has issued a revised federal qualification number, N-1-02-21-21-003, to the Unity 2.4.3.1 system.

The IRM version 6.4.3.3 is approved for use in California. Further IRM 6.4.3.0 must be replaced with 6.4.3.3 in all counties using Unity 2.4.3, updating to Unity 2.4.3.1.

Sincerely,

BRUCE MCDANNOFF
Interim Director
Office of Voting Systems Technology Assessment

ES&S Detailed Response to the California Secretary of State Conditions for the Use of ES&S' Optical Scan Voting Systems

Item 1: Clean Installation of Applications:

SoS Condition: Before any use in the February 5, 2008, Presidential primary election, jurisdictions must reinstall all software and firmware (including reformatting all hard disk drives and reinstalling the operating system where applicable) on all election management system servers and workstations, voting devices and hardware components of the voting system. Voting system application software must be reinstalled using the currently approved version obtained directly from the federal testing laboratory or the Secretary of State.

ES&S Response: Jurisdiction Task – ES&S has already authorized the ITA Voting System Test Lab ("VSTL") to release the trusted build version to the California Secretary of State's office on a CD-Rom and identified the respective counties to which the SoS office can securely send the files. However, the County Election Administrators play a critical role in this process and they will be responsible for uninstalling and reinstalling the VSTL supplied firmware version onto their county's voting system units. Accordingly, ES&S appreciates the Secretary's recognition that under the circumstances, the counties are not in a position to timely accomplish this activity for purposes of the February 5, 2008 election and has waived this requirement for that election.

Item 2: Virus Protection Procedure

SoS Condition: Within 15 days the vendor must present a plan and jurisdiction Election Procedures to the Secretary of State for approval that will prevent future viral propagation of malicious software from one system component to another, such as from a voting system component located in one precinct to voting system components located in other precincts. The plan and Election Procedures must incorporate, or employ methods at least as effective as, a configuration of parallel central election management systems separated by an "air gap" where (1) a permanent central system known to be running unaltered, certified software and firmware is used solely to define elections and program voting equipment and memory cards, (2) a physically-isolated duplicate system, reformatted after every election to guard against the possibility of infection, is used solely to read memory cards containing vote results, accumulate and tabulate those results and produce reports, and (3) a separate computer dedicated solely to this purpose is used to reformat all memory devices before they are connected to the permanent system again. (This "air gap" model was proposed by the Source Code Review Team that reviewed the Diebold Election Systems, Inc., GEMS 1.18.24 voting

system. Further details concerning the model are provided in Section 6.10 of the Source Code Review of the Diebold Voting System, dated July 20, 2007, and available on the Secretary of State website at:

<http://www.sos.ca.gov/elections/voting~systems/ttbr/diebold-sourcepublic-jul29.pdf>.

ES&S Response: ES&S will incorporate the following virus protection steps into our Voting System Election Procedures for California counties, which is currently in the process of being updated. ES&S will work with each of our county customers to gain their input prior to submitting our final recommendations, as the chain of custody and end-to-end process for securing the county voting system is solely the responsibility of the county election officials.

ES&S recommends the following procedures be used by all jurisdictions:

- 1) Three separate PCs configured as detailed in "standard configuration" shall be used in stand-alone (**non-networked**) mode and secured in an appropriate manner to assure controlled access and maintain chain of custody records:
 - a. the first PC (the "Election Definition PC") shall be used only to define the election and to load the memory devices that are used in the voting devices
 - b. the second PC (the "Election Reporting PC") shall be used only for collection and reporting of the election results
 - c. c) the third PC (the "Media Cleaning PC") shall be used only to clear/reformat the memory devices following the election and before the next election usage
- 2) The specified configuration includes commercially available and standard virus detection software. Virus detection software must be installed and enabled on all three of the referenced PCs at all times and removable media must always be scanned by the configured PC to prevent virus entry and propagation. The virus detection software must be kept current and up-to-date by establishing a periodic check by the responsible county election official.

Item 3: Reformatting of Electronic Media

SoS Condition: To prevent potential viral propagation of malicious software that could be introduced through an AutoMARK device, all memory cards used in the AutoMARK devices to configure them for an election must be

reformatted by a physically and logically isolated computer using commercial software (not developed by ES&S) before the memory card can be reinserted into any other component of the voting system during that election or any subsequent election.

ES&S Response: This is a county level responsibility. – **The local Election Authorities** have ability to perform this task. Or they could contract this work to ES&S and/or a third party if necessary.

Item 4 – Part I: Hardware and Operating System Configuration Specification and Hardening

SoS Condition: Within 15 days the vendor must submit to the Secretary of State for approval specifications for the hardware and operating system platform that must be used for all applicable components of the voting system. The vendor must identify the requirements for "hardening" the configuration of that platform, including, but not limited to:

- BIOS configuration;
- Identification of essential services that are required and non-essential services that must be disabled;
- Identification of essential ports that are required and non-essential ports that must be disabled and, if feasible, removed or physically blocked;
- Audit logging configuration;
- Definition of user security roles and associated permissions to assure all users have only the minimum required permissions for their role;
- Password policies, including password strength, expiration, and maximum attempts, along with all related user account control settings; and
- All utilities and software applications, with specifications for their installation, configuration and use, that are necessary for operation of the voting system (e.g., security software, data compression utilities, Adobe Acrobat, etc.).

ES&S Response: The Unity 2.4.3.1 Configuration is specified in the appropriate Federal and State Certification documents on file with the State of California. Certification was achieved on Windows XP Pro SP1. ES&S submits that XP SP2 with all current security updates and security patches is a more desirable solution and is assigning resources to test Unity 2.4.3.1 on XP Pro SP2. On successful completion of these tests, the Secretary of State,

with guidance from the counties, will have the option of allowing counties a variance and ability to upgrade.

In addition, ES&S will download and test configurations as defined in the specification for "Specialized Security – Limited Functionality" by the Center for Internet Security (CIS – www.cisecurity.org) in its Windows XP Professional Benchmark Consensus Baseline Security Settings. The CIS is a consortium dedicated to securing government, private, and public technical infrastructures and their website has tools available for accomplishing this point. ES&S is not authorized or allowed to distribute these tools, but highly recommends their use and can provide direction and guidance for their use. The full procedure, when tested and made available after the February 5th election, would have the following basic form:

- 1) Each PC must be cleaned and loaded with Windows XP Professional SP2 at the latest patch level;
- 2) Virus Detection software would then be installed on the PC;
- 3) Each PC would be configured as defined in the specification for "Specialized Security – Limited Functionality" by the Center for Internet Security (CIS) in its Windows XP Professional Benchmark Consensus Baseline Security Settings.
- 4) Loading of Applications:
 - a. Load the Election Definition PC with the Unity suite components for defining elections: EDM, ESSIM, and HPM.
 - b. Load the Election Reporting PC with the Unity suite component for reporting election results: ERM.
 - c. Load the Media Cleaning PC with the preferred 3rd party application for formatting election data storage media.

To the extent not already included, ES&S will further incorporate these points into any updates to its California Election Procedures, a current draft of which is enclosed with these responses.

Item 4 – Part II: Automated Configuration Verification Utility

SoS Condition: The vendor must identify automated mechanisms for jurisdictions to confirm and document that their system has been configured to these standards, and that all updatable components are the approved

version and level. The vendor must provide full instructions for the use of these mechanisms, including expected results.

ES&S Response: ES&S is investigating a validation utility from the Center for Internet Security (“CIS”) that would be used to check the configuration of the PC. ES&S will download and test this utility and upon approval from the Secretary of State, will work with the County Election Administrators to develop a procedure for its installation and use.

In addition, ES&S has a utility that was developed for newer versions of the Unity Software that will report a file hash for each application file that can then be compared with the approved hashes published with the certification to verify that all appropriate files are present and unaltered. On successful completion of these tests and upon approval from the Secretary of State, ES&S will work with the County Election Administrators to develop a procedure for its installation and use following the February 5th election.

Item 5: Post Repair/Modification Integrity Verification Procedure

SoS Condition: Immediately after any repair or modification of any voting system component that requires opening the housing, the integrity of the firmware and/or software must be verified using the automated mechanisms described above, or all software must be reinstalled by the jurisdiction from a read-only version of the approved firmware and/or software supplied directly by the federal testing laboratory or Secretary of State before the equipment can be put back into service.

ES&S Response: This is a jurisdictional task, which must be controlled by each County Election Administrator -- Jurisdictions have ability to perform this security step. ES&S will support this task by providing a best practices process and activity log form for use by the county during any repair, modification or preventative maintenance activity. ES&S will authorize the VSTL to provide this firmware version directly to the California Secretary of State’s office for distribution in a secure manner to all respective counties.

ES&S will adhere to this procedure and advise all of our technical support staff, via a technical advisory bulletin, to support the local California County Election officials in this best practices task.

Item 6: Prohibit Non-Approved Software on Voting Equipment

SoS Condition: Jurisdictions are prohibited from installing any software applications or utilities on any component of the voting system that have not been identified by the vendor and approved by the Secretary of State.

ES&S Response: This is a jurisdictional task.

Item 7: Security Patch Procedure

SoS Condition: Within 15 days the vendor must develop and submit to the Secretary of State for approval, a plan and procedures for timely identification of required security updates (e.g., operating system security patches, security software updates, etc), vendor testing of the updates, and secure distribution and application of vendor approved security updates.

ES&S Response: ES&S recommends the following overall guidelines be followed, assuming the Secretary of State's office authorizes in writing that such infrastructure updates do not require a further approval at the state level:

- The configuration of any and all PCs that will be used in the election must not be changed other than by the jurisdiction's IT system administrator and then only with express approval of the jurisdiction supervisor or election administrator.
- Security patches (and periodic updates) to the OS and the Virus Detection software may be required. Such changes must meet the same criteria, i.e., they are only applied by the jurisdiction's IT system administrator and only with express approval of the jurisdiction supervisor election administrator.
- Prior to their installation, all updates must be validated as true patches using their digital hashes on file with the provider and/or the National Software Reference Library ("NSRL").
- ES&S will, as a standard practice, review all security update notices published by the operating system and virus detection vendors and make any necessary periodic recommendations to the California SOS and to all local county jurisdictions on the need to patch the systems as part of periodic technical advisory updates.
- ES&S will perform periodic reviews on release of vendor notices.
- ES&S shall test all patches prior to recommending them for incorporation.
- ES&S will provide recommendations to the California SOS and to all local jurisdictions within 90 days of initial notice from the vendor, or inform the SOS and the jurisdiction of reasons for any extended review period.

To the extent not already included, ES&S will further incorporate these points into any updates to its California Election Procedures, a current draft of which is enclosed with these responses.

Item 8: Physical & Logical Security Proc Doc

SoS Condition: Within 15 days the vendor, working with elections officials, must develop and submit to the Secretary of State for approval, requirements and Election Procedures for operating and maintaining the physical and logical security of the system, including, but not limited to:

- Physical security and access to the system and all components;
- Network security;
- Data security (including data backup requirements and procedures); and
- Separation of roles and responsibilities for jurisdiction personnel.

ES&S Response: Many of the requirements under this point are dictated or provided by legislation, the California Secretary of State's office, and the United States Election Assistance Commission's election best practices guidelines and are already published and followed by the particular counties in their respective election procedures manuals. ES&S is reviewing the applicable directives from the State and has requested the respective individual counties' election procedures to allow these best practices to be included in the Election Procedures, which is in progress of being updated and will be provided to California Secretary of State for approval pursuant to item 28

Item 9: Network Limitations Requirement

SoS Condition: No network connection to any device not directly used and necessary for voting system functions may be established. Communication by or with any component of the voting system by wireless or modem transmission is prohibited at any time. No component of the voting system, or any device with network connectivity to the voting system, may be connected to the Internet, directly or indirectly, at any time.

ES&S Response: This task is under the control and within the responsibility of the County Election Administrator, and not ES&S.

Item 10: Detailed Use & Test Procedures

SoS Condition: Within 15 days the vendor, working with elections officials, must develop and submit to the Secretary of State for approval, detailed requirements and Election Procedures for programming, pre- and post-election logic and accuracy testing, transporting and operating voting equipment that will prevent or detect unauthorized access to or modification of any component of the voting system, including, but not limited to:

- Chain of custody controls and signature-verified documentation;
- Requirements for secure interim storage of any system component; and
- Employment of mechanisms to detect unauthorized access to the equipment.

At a minimum, the Election Procedures must require the jurisdiction to secure all voting system components in one or more uniquely serialized, tamper-evident container(s) before the jurisdiction transfers them to the custody of an Inspector, other poll worker, drayage company or other intermediary, or before jurisdiction personnel deliver them to a secure polling place or secure satellite distribution facility, as the case may be. Transportation of voting system components to the custody of an Inspector, other poll worker, drayage company or other intermediary, secure polling place, or secure satellite distribution facility shall not occur earlier than 10 calendar days prior to Election Day. Electronic components of a voting system not transported back to the jurisdiction headquarters on election night must be secured in one or more uniquely serialized, tamper-evident container(s) and placed in secured storage. The Election Procedures must impose the same requirements for signed logging of the inspection of security containers and the removal and return of voting system components to security containers that apply to security seals and locks on the voting system components themselves. The following are examples of acceptable tamper evident containers:

- A uniquely serialized, sealed banker's bag;
- A zippered nylon or canvass bag or case on which the zipper(s) that prevent access to the voting system component(s) inside are kept closed by a uniquely serialized, tamper-evident lock; or
- A hard lid that blocks access to all doors, ports or other points of access to the inside of the voting system component(s) and that is held in place by a latch or latches closed with a uniquely serialized, tamper-evident lock or locks.

The Election Procedures must also require a minimum of two elections officials or poll workers to perform or directly observe critical security processes, such as sealing and locking equipment for transport, conducting logic and accuracy testing, verifying the integrity and authenticity of security locks and seals, setting up voting equipment, opening the polls, closing the polls and printing results.

ES&S Response: ES&S is in the process of developing these Election Procedures, but notes that these “election best practices” are already part of steps the United States Election Assistance Commission has offered to all State and County election officials as recommendations to follow. Much of the

"What is required" is also covered by the procedures published by the Election officials of the State and Counties. The "how" to run the equipment is already covered by ES&S documents that have been filed as part of the California Certification process in our technical data packages and in turn should be shared with each California County Election Administrator.

Further, ES&S does offer, as presented on our web site, a variety of items all intended to allow the County Election Administrator to apply their level of local security and control as required. For instance, there are a variety of seals and a "Jackson Lid"¹ which can be used to assist in this chain of custody process that each respective county election administrator can apply for his or her county.

To the extent not already included, ES&S will further incorporate these points into any updates to its California Election Procedures, a current draft of which is enclosed with these responses.

Item 11 - Part A: Tamper Seal Serialization Requirement

SoS Condition: Where application of tamper-evident seals directly to a system component is required to detect unauthorized access to the component, those seals must be serialized

ES&S Response: This is the role and responsibility of the County Election Administrator. ES&S notes that these "election best practices" are already part of steps that the United States Election Assistance Commission has offered to all State and County election officials as recommendations to follow. Much of the "What is required" is also covered by the procedures already published by the election officials of the State and Counties.

Finally, there are a variety of seals which can be used to assist in this chain of custody process

Item 11 - Part B: Tamper Seal Specification

¹ The optional M100 Security Lid, or "Jackson Lid", can be used to prevent unauthorized access to the M100 while it is mounted on the ballot box. After the M100 is mounted to the top of the ballot box, the security lid can be placed over the unit. When the door that holds the M100 into place is locked, the security lid cannot be removed. Once the lid is in place, it prevents access to all operational components of the system, and covers up the ballot input tray and ballot insertion slot. Enclosed as Exhibit B are photographs of the optional M100 Security Lid.

SoS Condition: The vendor must specify in each instance the type of the seal to be used and the exact placement of that seal using photographs.

ES&S Response: ES&S is reviewing the seals currently used by each jurisdiction against the State requirements. In order to fully and effectively respond to this item, however, each county election administrator will have to share his or her past practices and thoughts regarding security and the chain of custody over the county's voting system. Security seals are commercially available from a number of sources and the seals to be used by each county needs to be determined by their respective County Election Administrators, based upon their particular requirements for managing their own election security practices.

Item 12: Public Inspection Requirement

SoS Condition: Upon request, members of the public must be permitted to observe and inspect, without physical contact, the integrity of all externally visible security seals used to secure voting equipment in a time and manner that does not interfere with the conduct of the election or the privacy of any voter.

ES&S Response: This is a responsibility of the County Election Administrator.

Item 13: Poll Closing/ Reporting Procedure

SoS Condition: Where voting equipment is used to record and tabulate vote results in a polling place, upon close of the polls, the poll workers are required to print two copies of the accumulated vote results and one audit log from each device. Each poll worker must sign every copy. One copy of the vote results from each device must be publicly posted outside the polling place. The second copy, along with the audit log, must be included with the official election material that is returned to the jurisdiction headquarters on election night.

ES&S Response: This is a responsibility of the County Election Administrator.

To the extent not already included, ES&S will further incorporate these points into any updates to its California Election Procedures, a current draft of which is enclosed with these responses.

Item 14: Voter Privacy

SoS Condition: No poll worker or other person may record the time at which or the order in which voters vote in a polling place.

ES&S Response: This is the responsibility of the County Election Administrator.

Item 15: Post Election Audit Personnel Requirements

SoS Condition: Poll workers are not permitted to participate in any post-election manual count auditing of precinct results from a precinct in which they were a poll worker.

ES&S Response: This also is the responsibility of the County Election Administrator.

Item 16: Post Election Audit Procedures

SoS Condition: Within 15 days the vendor, working with elections officials, must develop and submit to the Secretary of State for approval, specific detailed requirements and Election Procedures for vote results auditing and reconciliation, review of audit logs and retention of election documentation to validate vote results and detect unauthorized manipulation of vote results, including, but not limited to:

- Precinct level ballot accounting;
- Identification of abnormal voting patterns on ballots printed by AutoMARK voter assist terminals; and
- Reconciliation of variances between electronic and manual audit vote results.

ES&S Response: Some requirements under this point are already dictated by State election law and already published and followed by the particular jurisdictions in their respective procedures manuals. ES&S is therefore reviewing the applicable directives from the State and the individual county procedures in order to make proposals consistent with existing law and to allow these best practices to be included in its Election Procedures, which is in process.

To the extent not already included, ES&S will further incorporate these points into any updates to its California Election Procedures, a current draft of which is enclosed with these responses.

Item 17: Vendor Pays for Post-Election Audit

SoS Condition: Any post-election auditing requirements imposed as a condition of this certification shall be paid for by the vendor. Elections officials are required to conduct the audits and the vendor is required to reimburse the jurisdiction.

ES&S Response: ES&S respectfully submits the Secretary's Office lacks statutory authority to impose this condition. Instead, any obligation by ES&S to engage in, or pay for post-election services is governed by the terms of its hardware sales contract and any annual service contracts with each individual county customer. Otherwise, additional costs would be imposed that were never contracted for by ES&S and its county customers. Without waiver of its position, ES&S can offer support services and election services if a county wishes to enter (or has entered) a contract to provide them.

Item 18: Post Election Manual Count Requirements

SoS Condition: After consultation with elections officials, the Secretary of State shall establish additional post-election manual count auditing requirements, including:

- Increased manual count sample sizes for close races, based on an adjustable sample model, where the size of the initial random sample depends on a number of factors, including the apparent margin of victory, the number of precincts, the number of ballots cast in each precinct, and a desired confidence level that the winner of the election has been called correctly. In establishing sampling requirements for close races, the Secretary of State may impose a specific sampling threshold for a given vote differential or percentage of the margin of victory, taking into account the number of electors and the number and size of precincts in the race;
- Escalation requirements for expanding the manual count to additional precincts when variances are found; and
- Procedures to increase transparency and effectiveness of post-election manual count audits.

Elections officials must comply with additional post-election manual count auditing requirements as set forth by the Secretary of State in the document entitled "Post-Election Manual Tally Requirements" and any successor document.

The vendor shall reference compliance with the "Post-Election Manual Tally Requirements" in its Election Procedures for the voting system

ES&S Response: ES&S respectfully submits that the Secretary's Office lacks authority to impose additional post-election manual count auditing requirements that are not otherwise authorized by statute or appropriately enacted pursuant to the California Administrative Procedures Act. ES&S will, of course, incorporate into its Election Procedures those requirements that are properly authorized under California statutes, rules or regulations.

Item 19 – Part A: Vendor Provides Test Ballots & Calibration Proc (550's & 650's)

SoS Condition: Paragraph 5(g) of the Conditional Approval of Use of Election Systems and Software, Inc. Optical Scan Voting System issued on August 3, 2005, requires the vendor to provide all users of this system with test ballots and appropriate procedures to check and assess calibration of the Model 550 and Model 650 central tabulation scanners prior to each election.

ES&S Response: ES&S makes all necessary materials available to customers, at the customer's expense in accordance with our contractual obligations. Calibration Procedures for the Model 550 and Model 650 central tabulation scanners are only performed by trained and authorized ES&S technicians.

Item 19 – Part B: Vendor Provides Test Ballots & Calibration Proc (M100)

SoS Condition: Vendor is hereby required to provide all users of this system who use the Model 100 precinct tabulation counter scanners with test ballots and appropriate procedures to check and assess calibration of the Model 100

ES&S Response: ES&S makes all necessary materials available to customers, at the customer's expense in accordance with our contractual obligations. Calibration Procedures are already in place and being used by counties.

Item 19 – Part C: Pre/Post Calibration Test Requirements

SoS Condition: In addition, Elections officials must check and assess calibration of each Model 100, Model 550 and Model 650 scanner unit both before each election and following each election before the end of the official canvass.

ES&S Response: This is the responsibility of the County Election Administrator. ES&S can contract to support this as part of pre- and post-election logic and accuracy testing performed by Jurisdictions.

Item 19 – Part D: Vendor Pays for Post-Election Calibration Testing

SoS Condition: The vendor is required to reimburse the jurisdiction for the cost of the post-election calibration testing.

ES&S Response: ES&S respectfully submits the Secretary's Office lacks statutory authority to impose this condition. Instead, the terms of the county's contract with ES&S governs any obligation to pay for post-election calibration. Otherwise, costs would be imposed which were never contracted for by ES&S and its county customers. Without waiver of its position, ES&S can offer such a service if a county wishes to enter (or has entered) a services contract to provide it.

Item 20: Poll Issues Log

SoS Condition: Each polling place must be equipped with a method or log in a format specified by the Secretary of State after consultation with elections officials to record all problems and issues with the voting equipment in the polling place as reported by voters or observed by poll workers. Such records must include the following information for each event:

- Date and time of occurrence;
- Voter involved, if any;
- Equipment involved;
- Brief description of occurrence;
- Actions taken to resolve issue, if any; and
- Elections official(s) who observed and/or recorded the event

ES&S Response: This is a responsibility of the County Election Administrator.

Item 21: Publishing of Poll Issues Log

SoS Condition: All such event logs or reports must be made available to the public for inspection and review upon request. Prior to or concurrent with the certification of the election, the elections official must submit a report to the Secretary of State of all reported problems experienced with the voting system and identifying the actions taken, if any, to resolve the issues.

ES&S Response: This is a responsibility of the County Election Administrator.

Item 22: Pollworker Training

Training of poll workers must include the following:

- Secure storage of voting equipment while in the poll worker's possession;
- Chain-of-custody procedures required for voting equipment and polling place supplies;
- Seal placement and procedures for verification of seal integrity;
- Placement and observation of voting equipment;
- Observation of activity that could indicate tampering or an attempt at tampering;
- The Voter Bill of Rights set forth in section 2300 of the Elections Code;
- The nature of the AutoMARK voter assist terminal as a device that marks official paper ballots and, unlike a direct recording electronic (Dm) voting machine, does not create an electronic record of votes;
- The public right to inspect voting equipment and security seals, and how to handle requests for such inspection;
- How to handle lack of sufficient paper ballots or equipment failure in a polling place, including AutoMARK ballot jams or other AutoMARK operational problems, and how to ensure continuity of the election in the event of such a failure; and
- How to properly log all events and issues related to voting equipment in the polling place, including voter complaints of malfunctioning equipment.

ES&S Response: This is a responsibility of the County Election Administrator. ES&S could be contracted to perform this training if requested by a county customer.

Item 23: Public Inspection Requirement

SoS Condition: Elections officials must develop appropriate security procedures for use when representatives of qualified political parties and bona fide associations of citizens and media associations, pursuant to their rights under Elections Code section 15004, check and review the preparation and operation of vote tabulating devices and attend any or all phases of the election. The security procedures must permit representatives to observe at a legible distance the contents of the display on the vote tabulating computer or device. This requirement may be satisfied by positioning an additional display monitor or monitors in a manner that allows the representatives to read the contents displayed on the vote tabulating computer or device while also observing the vote tabulating computer or device and any person or persons operating the vote tabulating computer or device.

ES&S Response: This is a responsibility of the County Election Administrator.

Item 24: Paper Ballot Privacy Sleeve Requirement

SoS Condition: All voters voting on paper ballots in a polling place must be provided a privacy sleeve for their ballot and instructed on its use in accordance with Elections Code section 14272.

ES&S Response: Every AutoMARK voter assist terminal included a “privacy sleeve”² kit that the County Election Administrator could utilize in their election events. The kit included: a.) Braille instructions for the voter that is blind or visually impaired; b.) Velcro attachment pads; and c.) Two (2) ballot privacy sleeves. One kit per AutoMARK unit was shipped as part of the initial installation for any county utilizing the AutoMARK as their accessible voter device with their voting system. The ballot privacy sleeves are a consumable item that the County Election Administrator can re-order from ES&S. The use and application of the ballot privacy sleeve is covered in “ES&S AutoMARK” “California Election Procedures Manual for the ES&S AutoMARK Voter Assist Terminal”, a copy of which is being included with this response document.

Additionally the County Election Administrators can utilize these same privacy sleeves for any voter requesting one, or the County Election Administrators may elect to provide privacy envelopes to voters needing or requesting a ballot privacy sleeve.

Item 25: Tampering Law Warning in Booth

SoS Condition: A warning must be posted in each voting booth stating that, pursuant to Elections Code sections 18564,18565,18566,18567,18568 and 18569, tampering with voting equipment or altering vote results constitutes a felony, punishable by imprisonment.

ES&S Response: This is a responsibility of the County Election Administrator.

Item 26: Compromised Equipment Procedures

SoS Condition: With respect to any piece of voting equipment for which the chain of custody has been compromised or for which the integrity of the

² Enclosed as Exhibit C are photographs of a privacy sleeve.

tamper-evident seals has been compromised, the following actions must be taken: (See ES&S's responses to each sub point below.)

Item 26 Part A: Compromised Equipment Procedures – Notification Requirement

SoS Condition: The chief elections official of the jurisdiction must be notified immediately;

ES&S Response: This is a responsibility of the County Election Administrator.

Item 26 Part B: Compromised Equipment Procedures – Removal from Service

SoS Condition: The equipment must be removed from service immediately and replaced if possible;

ES&S Response: This is a responsibility of the County Election Administrator.

Item 26 Part C: Compromised Equipment Procedures – Manual Tally

SoS Condition: Any votes cast on the device prior to its removal from service must be subject to a 100% manual tally, by the process described in Elections Code section 15360, over and above the normal manual tally conducted during the official canvass as defined in Elections Code section 336.5.

ES&S Response: This is a responsibility of the County Election Administrator.

Item 26 Part D: Compromised Equipment Procedures – Memory Card Retention

SoS Condition: Any memory card containing data from that device must be secured and retained for the full election retention period;

ES&S Response: This is a responsibility of the County Election Administrator.

Item 26 Part E: Compromised Equipment Procedures – Software/Firmware Retention

SoS Condition: An image of all device software and firmware must be stored on write-once media and retained securely for the full election retention period;

ES&S Response: This is a responsibility of the County Election Administrator.

Item 26 Part F: Compromised Equipment Procedures – Reloading System

SoS Condition: All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.

ES&S Response: This is a responsibility of the County Election Administrator.

Item 27: Fatal Error Procedure

SoS Condition: With respect to any piece of voting equipment for which the chain of custody has been compromised or for which the integrity of the tamper-evident seals has been compromised, the following actions must be taken: (See ES&S's responses to each sub point)

Item 27 Part A: Fatal Error Procedure – Notification Requirement

SoS Condition: The chief elections official of the jurisdiction must be notified immediately;

ES&S Response: This is a responsibility of the County Election Administrator.

Item 27 Part B: Fatal Error Procedure – Removal from Service

SoS Condition: The equipment must be removed from service immediately and replaced if possible;

ES&S Response: This is a responsibility of the County Election Administrator.

Item 27 Part C: Fatal Error Procedure – Manual Tally

SoS Condition: Any votes cast on the device prior to its removal from service must be subject to a 100% manual tally, by the process described in Elections Code section 15360, over and above the normal manual tally conducted during the official canvass as defined in Elections Code section 336.5.

ES&S Response: This is a responsibility of the County Election Administrator.

Item 27 Part D: Fatal Error Procedure – Memory Card Retention

SoS Condition: Any memory card containing data from that device must be secured and retained for the full election retention period;

ES&S Response: This is a responsibility of the County Election Administrator.

Item 27 Part E: Fatal Error Procedure – Software/Firmware Retention

SoS Condition: An image of all device software and firmware must be stored on write-once media and retained securely for the full election retention period;

ES&S Response: This is a responsibility of the County Election Administrator.

Item 27 Part F: Fatal Error Procedure – Failure Analysis

SoS Condition: The vendor or jurisdiction shall provide an analysis of the cause of the failure;

ES&S Response: The jurisdiction may contract with the vendor to perform this service

Item 27 Part G: Fatal Error Procedure – Device Retention

SoS Condition: Upon request by the Secretary of State, the vendor or jurisdiction shall retain the device for a reasonable period of time to permit forensic analysis;

ES&S Response: Upon written request, the vendor will retain the device for a reasonable period of time.

Item 27 Part H: Fatal Error Procedure – Reloading System

SoS Condition: All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.

ES&S Response: This is a responsibility of the County Election Administrator, but ES&S is prepared to assist in accordance with any applicable contractual obligations.

Item 28: SOS Response Commitment of 15 Days

SoS Condition: The Secretary of State will review and finalize all plans, requirements and procedures submitted pursuant to the foregoing requirements above within 15 days of receipt. Upon approval, all such plans, requirements and procedures will automatically be incorporated into the official Election Procedures for the voting system, and will become binding upon all users of the system

ES&S Response: No ES&S Action.

Item 29: System Change Control

SoS Condition: No substitution or modification of the voting system shall be made with respect to any component of the voting system, including the Election Procedures, until the Secretary of State has been notified in writing and has determined that the proposed change or modification does not impair the accuracy and efficiency of the voting system sufficient to require a re-examination and approval.

ES&S Response: The Secretary's position is noted.

Item 30: SOS Right to change Cert Conditions

SoS Condition: The Secretary of State reserves the right, with reasonable notice to the vendor and to the jurisdictions using the voting system, to modify the Election Procedures used with the voting system and to impose additional requirements with respect to the use of the system if the Secretary of State determines that such modifications or additions are necessary to enhance the accuracy, reliability or security of any of the voting system. Such modifications or additions shall be deemed to be incorporated herein as if set forth in full.

ES&S Response: The Secretary's reservation is noted.

Item 31: Pre-Election Filing Requirements

SoS Condition: Any jurisdiction using this voting system shall, prior to such use in each election, file with the California Secretary of State a copy of its Election Observer Panel plan.

ES&S Response: This is a responsibility of the County Election Administrator.

Item 32 – Part A: Vendor Supply Full Voting System upon request (w/in 30 days)

SoS Condition: The vendor agrees in writing to provide, and shall provide, to the Secretary of State, or to the Secretary of State's designee, within 30 days of the Secretary of State's demand for such, a working version of the voting system, including all hardware, firmware and software of the voting system, as well as the source code for any software or firmware contained in the voting system, including any commercial off the shelf software or firmware that is available and disclosable by the vendor, provided that the Secretary of State first commits to the vendor in writing to maintain the confidentiality of the contents of such voting system or source code so as to protect the proprietary interests of the vendor in such voting system or source code. The terms of the commitment to maintain confidentiality shall be determined solely by the Secretary of State, after consultation with the vendor.

ES&S Response: Acknowledged, provided an appropriate confidentiality and non-disclosure agreement is executed between the parties in order to maintain the confidentiality of ES&S's proprietary information.

Item 32 – Part B: Software/Firmware Review at Vendor's Expense

SoS Condition: The voting system shall not be installed in any California jurisdiction until the vendor has signed such an agreement. Any reasonable costs associated with the review of the source code for any software or firmware contained in the voting system shall be born by the vendor.

ES&S Response: ES&S will pay for reasonable costs associated with the initial certification of a voting system or the reasonable costs of a certification for changes made by ES&S to the extent provided by law.

Item 33: SOS Election Monitoring

SoS Condition: The Secretary of State reserves the right to monitor activities before, during and after the election at any precinct or registrar of

voters' office, and may, at his or her discretion, conduct a random parallel monitoring test of voting equipment.

ES&S Response: ES&S notes the Secretary's reservation.

Item 34: Statement of Election Law

SoS Condition: By order of the Secretary of State, voting systems certified for use in California shall comply with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. Voting systems shall also comply with all state and federal voting system guidelines, standards, regulations and requirements that derive authority from or are promulgated pursuant to and in furtherance of California Elections Code and the Help America Vote Act of 2002 or other applicable state or federal law when appropriate.

ES&S Response: This does not require any response by ES&S at this time.

Item 35: Statement of Responsibility

SoS Condition: Voting system manufacturers or their agents shall assume full responsibility for any representation they make that a voting system complies with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. In the event such representation is determined to be false or misleading, voting system manufacturers or their agents shall be responsible for the cost of any upgrade, retrofit or replacement of any voting system or its component parts found to be necessary for certification or otherwise not in compliance.

ES&S Response: Any representation is governed by the vendor's contract with its customer.

Item 36: Statement of Election Law Requirement

SoS Condition: Any voting system purchased with funds allocated by the Secretary of State's office shall meet all applicable state and federal standards, regulations and requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002.

ES&S Response: This does not require any response by ES&S at this time.

Item 37: Establish CA County User Group

SoS Condition: The vendor must establish a California County User Group and hold at least one annual meeting where all California users and Secretary of State staff are invited to attend and review the system and ensure voter accessibility.

ES&S Response: ES&S has an established user group for California counties. ES&S will work with the county user group to coordinate with and apprise the Secretary of State's office of scheduled meetings assuring that the Secretary's staff has an opportunity to attend at least one of the meetings annually.

Item 38 – Part A: Provide Compile & Run Capability to CA Test Personnel

SoS Condition: In addition to depositing the source code in an approved escrow facility, the vendor must deposit with the Secretary of State a copy of the system source code, binary executables and tools and documentation, to allow the complete and successful compilation and installation of a system in its production/operational environment with confirmation by a verification test by qualified personnel using only this content.

ES&S Response: ES&S will agree to provide a copy of its voting system source code, executables, tools and documentation to the SOS as long as the SOS and ES&S can mutually agree on adequate procedures for handling ES&S's proprietary information, which would include, but not be limited to, confidentiality restrictions, license and use restrictions, and other procedures for the handling of proprietary information. However, ES&S notes that tools used to compile the Unity 2.4.3.1 version may no longer be commercially available. In addition, given that ES&S's Unity 3.0.1.1 system is currently pending certification by the Secretary of State's office; there should no longer be any need for such tools upon the certification and subsequent installation of this new voting system. ES&S requests an additional 30 days to make this available.

Item 38 – Part B: SOS Source Code Review

SoS Condition: The Secretary of State reserves the right to perform a full independent review of the source code at any time.

ES&S Response: ES&S may be agreeable to such a review, provided there is sufficient cause to conduct such a review, the confidentiality of the vendor's

information is maintained, and the cost of such review is borne by the State. It is ES&S's position that once a system is certified, it is unnecessary to continually review the system without reasonable cause.

Item 39 -- Paper Ballot Printing Specs & Printer Certification

SoS Condition: The vendor must provide printing specifications for paper ballots to the Secretary of State. The Secretary of State will certify printers to print ballots for this system based upon their demonstrated ability to do so. The vendor may not require exclusivity in ballot printing and must cooperate fully in certification testing of ballots produced by other ballot printers.

ES&S Response: This is already in place. Approved vendors and certification procedures are on the CA SoS Website.

Item 40 -- SOS Right to Change Certification Conditions

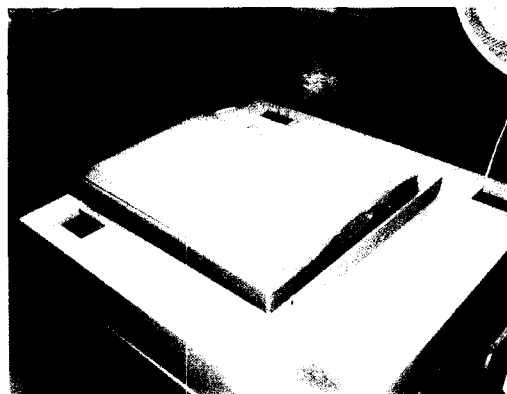
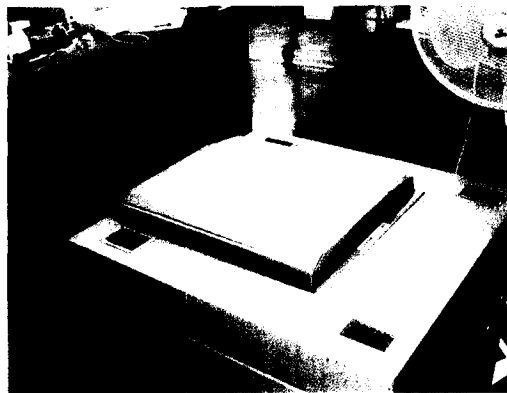
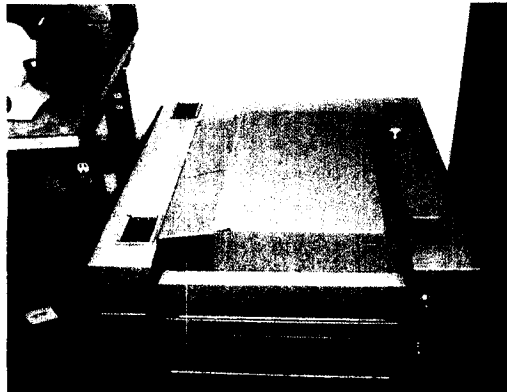
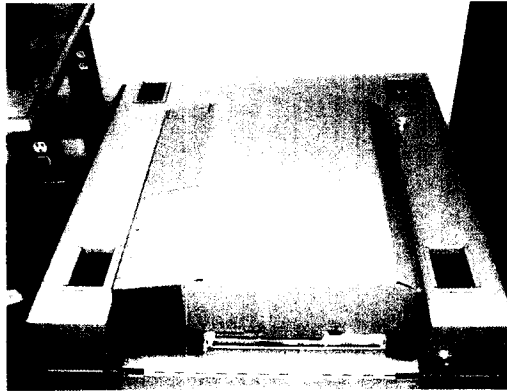
SoS Condition: Where circumstances require it, the Secretary of State may adjust or suspend any of the conditions of recertification for a vendor or a jurisdiction, as the Secretary of State deems prudent and necessary to facilitate successful election administration. Such adjustments or suspensions shall be deemed to be incorporated herein as if set forth in fill.

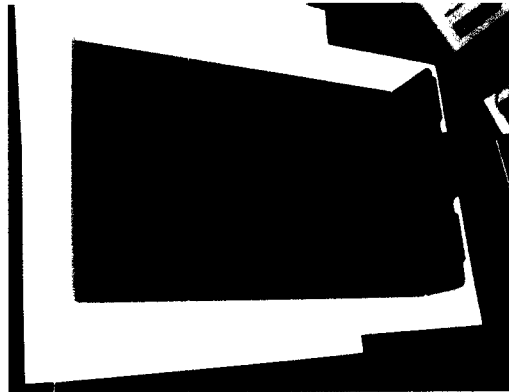
ES&S Response: This does not require any response from ES&S at this time, but ES&S reserves its right to seek adjustment or suspension of any condition pursuant to Item 40 or as provided by law.

NOTE: ES&S reserves the right to supplement or modify these responses.

Exhibit B

Security Cover Pictures





The optional M100 Security Lid can be used to prevent unauthorized access to the M100 while it is mounted on the ballot box. After the M100 is mounted to the top of the ballot box, the security lid can be placed over the unit. When the door that holds the M100 into place is locked, the security lid cannot be removed. Once in the lid is in place it prevents access to all operational components of the system, and covers up the ballot input tray and ballot insertion slot.



This Side
Down

This stamp intended for notices 1' to 14' long

Before Voting:

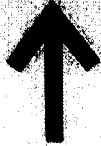
- Make sure the ballot is in the privacy sleeve.
- Firmly attach sleeves to ES&S AutoMARK using Velcro tabs.

The ES&S AutoMARK will automatically pull ballot into machine.

After Voting:

- ES&S AutoMARK returns ballot into privacy sleeve.
- Hold the sleeve by pressing firmly on the 'X' marks at the bottom nearest you.
- Pull sleeve and ballot from machine.
- When ballot is completely removed, take to the ballot box or counter to cast your vote.

If required, gently
push ballot into
machine



If required, gently
push ballot into
machine