

BOE in NYC
RFI for Voting System
Addendum # 2
Additional Security Questions
for
Election Systems & Software, Inc.

January 22, 2009

Table of Contents

Physical Security	2
Operating System Security	6
Data Security.....	10
Network Security	13
Application Development Security.....	15
Application Functional Security	19
Miscellaneous	26

Please answer each question for ALL major components of your proposed solution. Major components include the proposed Election Management System (EMS), the proposed Pollsite Voting System and the proposed Disability Voting Solution (if separate device).

Physical Security

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>1) Describe in detail the physical protection mechanism for each of the following (if key locks are indicated please provide information regarding lock type, keys duplication both on one machine and across multiple machines)</p> <ul style="list-style-type: none"> a) Storage containing operating system (Technology, Interface Form factor, location, physical segregation, etc) b) Storage of vote results (Technology, Interface Form factor, location, physical segregation, etc) c) Storage of election information and ballot definitions. d) Printer for results and status messages 	<p>The EMS runs on a PC under the Windows XP Operating System. The OS is resident on the PC hard drive.</p> <ul style="list-style-type: none"> a) The protections for this OS include lockdown of the BIOS and maintaining the PC in a physically controlled location. Other controls to protect the PC include hardening of the Windows OS so that only authorized users can log in and so that only authorized system administrators can perform administrative functions. b) Vote results are stored on the EMS PC on its hard drive, which is protected as described above. c) Election information and ballot definitions on the EMS PC are stored on its hard drive, which is protected as described above. d) The EMS PC prints results and status messages on a printer attached to the PC. The controls for this printer are those garnered from maintaining the PC in a physically secure environment. 	<p>DS200 operates from an imbedded Linux OS stored on a CF card enclosed within the case of the unit.</p> <ul style="list-style-type: none"> a) Controls for protecting the compact flash card that holds the OS include the need to remove the shell in order to access it. Additionally, physical controls to restrict the device from access by those not so authorized must be utilized. b) Vote results on the DS200 are stored on the USB memory stick that is physically locked behind a key-lock door. Vote records are digitally signed. c) Election information and ballot definitions are sent to the DS200 on the USB memory stick that is physically locked behind a key-locked door. The information is digitally signed to ensure its authenticity. d) The DS200 has a built-in printer that resides behind a key-lock door. 	<ul style="list-style-type: none"> a) This unit does not use a general-purpose PC. It uses an embedded processor on a custom single board computer. The OS is a custom configuration created by a Microsoft partner company. It is not accessible or updatable by the user. b) This is a BMD. There is no storage of vote totals. c) The compact flash card with election information is behind a key-locked panel. d) The printer that is used for all printing is integral to the unit and accessible only by removing covers. There is no internal paper storage. All printing, whether a voted ballot or log, requires insertion of a ballot or a sheet of paper.

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>2) Are redundant storage facilities available within the system, i.e. does the OS have a backup for hot swap, is there a backup for vote results storage?</p>	<p>Operating procedures should include periodic backup of the information on the EMS PC. The system administrator should schedule these with the election administrator.</p> <p>Documented procedures exist for clean reinstall of the OS, should it be required.</p>	<p>Procedures exist to allow for swap-out of the DS200 unit should it be required. Vote results from the initial unit exist on its USB memory stick and are retained. They can be merged for polling location reports.</p>	<p>VAT can be swapped out at any time with another unit. All OS and firmware storage uses non-volatile solid state memory. There is no redundant storage. The unit does not contain or store any vote results.</p>
<p>3) What physical security controls are in place to protect systems from being modified between the time the systems are built and the time they are delivered to the client?</p>	<p>N/A -- COTS PC.</p>	<p>Ricoh Electronics Incorporated (REI) manufacturing facilities in Tustin, CA have tightly controlled security procedures in place. There is a security guard at each entry gate, and access to the manufacturing and shipping areas is strictly enforced through the use of security badges and authorization lists. Shipments from the Tustin facility are transported by bonded freight carriers, and the loads are sealed with a recorded seal number. When the load arrives in Albany for acceptance testing, the ES&S representative cuts the seal after verifying the seal number shown on the bill of lading paperwork. Security of the units in the Albany warehouse is maintained by ES&S and SBOE staff during business hours and by roving security patrols during non-business hours. When the equipment passes acceptance testing by the SBOE, it is then repacked, sealed and loaded onto a bonded freight carrier who transports the units in a sealed and locked trailer to the end user client. Physical chain of custody is not broken from manufacturing through delivery of the items to the client.</p>	
<p>4) Please list all ports on the unit with descriptions of form factors, communication protocols and purpose</p>	<p>Using a standard COTS PC, the only required ports are the USB drive for the DS200 USB memory sticks and the compact flash reader, a printer port, a mouse and a keyboard. Any other ports are optional, at the manufacturer's control.</p>	<p>The DS200 OS is located on a compact flash port inside the DS200 shroud covering. Access to the compact flash port requires the removal of four screws with a Torx screwdriver, unlocking the front access door, and then removing the shroud from the DS200.</p>	<p>The port for the compact flash card is located under a key-lockable panel. A card must be installed in the port before the system can be used.</p> <p>No USB ports are externally available. The cover must be removed to access them. The cover also can be secured with seals.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
		<p>There are three USB ports inside the lockable front access door and one additional USB port in the lockable rear access door. Access to all four of these USB ports requires a key to gain access to the access door compartments.</p> <p>There is one additional USB port on the rear of the DS200. Access to the rear USB port is denied when the DS200 is installed inside the ballot box.</p> <p>Physical security of all ports can be enhanced by locking the DS200 inside the ballot box.</p> <p>Election jurisdictions can further safeguard the ports by placing seals over the front and rear access doors of the DS200 as well as the top lid of the ballot box.</p> <p>There is a modem jack inside the lockable rear access door. This port is not connected to any transmitter because no modems will be installed in the NY DS200 units.</p>	<p>The port is not active until the firmware enables it.</p> <p>An RJ45 connector is present, but no electronic connections to it are present.</p> <p>An audio plug is used for ADA headphones.</p> <p>A two-switch connector is used for an ADA two-switch device for ballot navigation control.</p> <p>An optional one-way USB port plugs into the internal USB and has the same limitations.</p>
<p>5) What capability is in place to secure ports from access by unauthorized connections, e.g. connecting a portable computing unit to the ports</p>	<p>For the EMS PC, we rely on physical device control, hardening the BIOS and the OS to disable the ports and services that aren't needed.</p>	<p>As stated in 4) above, access to all ports on the DS200 is denied when the unit is installed in the ballot box and when the front and rear access doors are locked and sealed.</p>	<p>There is a sealable, key-locked door for the compact flash card and a location for a seal for the rear USB port and ink cartridge access door. (See answer to 4 above.)</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
		<p>The DS200 firmware checks for a USB device and vendor ID from every device plugged into a USB port and denies access to all devices that do not match a list of known trusted devices. At this time, these devices are restricted to USB memory stick holding either public/private key pairs, election data or firmware updates.</p>	
<p>6) Are all modular and removable components (such as printers and memory modules) serialized to track system assemblies and sub assemblies?</p>	<p>Not applicable. The EMS PC is a COTS device and any serialization is at the prerogative of the manufacturer.</p>	<p>The DRAM, compact flash card, motherboard, printer board, USB hub board, power management board, and scanner board are all serialized. REI tracks the individual serial numbers of these assemblies and subassemblies in a database in accordance with their ISO 9000 procedures.</p>	<p>The AutoMARK SBC board is serialized with a unique number label on the board that is tracked by REI to identify the lot, date, and sequential number in accordance with their ISO 9000 procedures.</p>

Operating System Security

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>1) What is the underlying operating system? Detail the manufacturer, version, build and all relevant updates and patches.</p>	<p>OS Name: Microsoft Windows XP Professional</p> <p>Version: 5.1.2600 Service Pack 3 Build 2600</p> <p>Updates and Patches The specific updates applied to Service Pack 3 during the system hardening process are:</p> <ul style="list-style-type: none"> • WindowsXP-KB936929-SP3-x86-ENU.exe • WindowsUpdateAgent30-x86.exe • WindowsXP-KB942288-v3-x86.exe • ie7-windowsxp-x86-enu_d39b89c360fbaa9706b5181ae4718100687a5326.exe <p>Further detail on the updates and patches applied resides in the system log file and the log is available from ES&S upon request.</p>	<p>The DS200 employs a “built from scratch” Linux operating system with the 2.6.16.27 version kernel. The base instructions and materials for the OS come from the Linux From Scratch organization version 6.2 available from http://www.linuxfromscratch.org/ A VSTL has performed a trusted build of the operating system employed on the DS200, and all source files are publicly available</p>	<p>The OS is Windows CE version 5.00.19 created by EuroTech, a Microsoft partner. It has Microsoft Windows CE 5.0 as its kernel with added drivers to configure it to the requirement. Drivers are Microsoft modified, Microsoft unmodified or created by EuroTech. The version number fully specifies the implemented configuration.</p>
<p>2) Is there a standardized process for hardening of operating system components prior to delivery to the board of elections?</p> <p>a) What is the process for hardening the operating systems?</p> <p>b) Is the process available for public review?</p> <p>c) What is the process for validating that the</p>	<p>Yes, there is a standardized process for hardening the EMS PC’s OS documented by ES&S. This document is part of the ES&S Technical Data Package submitted for all State of NY certification events.</p> <p>a) The process for hardening the</p>	<p>The DS200 operates on an imbedded, customized Linux OS.</p> <p>a) & b) Hardening is done in the development of the certified deployment and is not modifiable.</p> <p>c) A validation process is documented to allow the user to validate that the OS on the device</p>	<p>a) & b) The VAT operates on an imbedded Windows CE OS that is customized to the device. It is not accessible to the user.</p> <p>c) A process is documented to allow the user to validate that the OS on the device matches the certified one.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>process is adhered to?</p>	<p>EMS PC's is documented in detail in the ES&S System Hardening Document. Essentially, it involves locking down all unneeded Windows services and disabling unneeded ports and connections.</p> <p>b) Yes.</p> <p>c) There is a documented validation process, included in the ES&S Hardening Document, that lets the user check validate that each EMS PC has been correctly hardened.</p>	<p>is the certified one.</p>	
<p>3) What is the mechanism and process used to install the operating system?</p>	<p>The Windows XP OS is loaded and hardened by the system administrator. A certified install disk for the Windows OS must be used to perform a clean install, and then the updates/patches and hardening process must be followed.</p>	<p>Initial/Clean Install</p> <p>During the REI manufacturing process, the DS200 OS is imaged by REI from a certified and controlled master image file.</p> <p>Update Process</p> <p>Currently any certified update to the OS requires the internal compact flash card to be removed from under the front cover of the unit. A certified master image is then written to the card; it is validated against the official signature or hash and returned to the unit.</p> <p>ES&S is very near completion of a method to update the OS using a USB memory stick that would eliminate the need to remove the</p>	<p>Initial Install</p> <p>The unit as manufactured contains an OS. It is contained on the flash chips assembled on the CPU board when the CPU board is manufactured.</p> <p>Update Process</p> <p>This OS may be reloaded from the compact flash card by removing the covers, attaching a USB keyboard and accessing the installed OS. OS routines can then be invoked to install the replacement OS.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
		front cover. Current plans call for finishing this update process in the month of February 2009.	
<p>4) How are announced security vulnerabilities addressed?</p> <p>a) Is there a formalized risk assessment process to review OS vulnerabilities as they are announced?</p> <p>b) What is the process for testing patches and/or hotfixes identified as required by the risk analysis process?</p> <p>c) Are results of this risk analysis published publicly?</p> <p>d) What is the process for deploying patches to systems as needed?</p> <p>e) Describe the process for validating that appropriate patches and fixes have been deployed</p> <p>f) How is the need for patches and updates addressed through the certification/recertification process?</p>	<p>a) ES&S monitors security alerts on a daily basis for impacts to its voting systems.</p> <p>b) When vulnerabilities are found, ES&S determines proper countermeasures, modifies its systems to include them and notifies its clients of these vulnerabilities and countermeasures.</p> <p>c) ES&S uses technical bulletins to document special procedures that clients should use for technical issue mitigation, including security issues to which permanent fixes have not yet received certification.</p> <p>d) All changes, including patches to the EMS and embedded firmware in the DS200 and AutoMark, are subject to federal and state certification events. It is the determination of the NYSBOE if patches to Windows desktop and server OS must be certified by NYSBOE before deployment and application to local BOE systems.</p> <p>e) In regards to patches applied</p>	<p>a) ES&S monitors security alerts on a daily basis for impacts to its voting systems.</p> <p>b) When vulnerabilities are found, ES&S determines proper countermeasures, modifies its systems to include them and notifies its clients of these vulnerabilities and countermeasures.</p> <p>c) ES&S uses technical bulletins to document special procedures that clients should use for technical issue mitigation, including security issues to which permanent fixes have not yet received certification.</p> <p>d) The current federal certification system does not have a specific method for implementing patches. All changes to the firmware or operating system are currently treated as complete updates to the system.</p> <p>e) Any patch or update is handled through the jurisdiction's certification process. Any altered firmware or OS would require an update signature as captured</p>	<p>a) ES&S monitors security alerts on a daily basis for impacts to its voting systems.</p> <p>b) When vulnerabilities are found, ES&S determines proper countermeasures, modifies its systems to include them and notifies its clients of these vulnerabilities and countermeasures.</p> <p>c) ES&S uses technical bulletins to document special procedures that clients should use for technical issue mitigation, including security issues to which permanent fixes have not yet received certification.</p> <p>d) The current federal certification system does not have a specific method for implementing patches. All changes to the firmware or operating system are currently treated as complete updates to the system.</p> <p>e) Any patch or update is handled through the jurisdiction's certification process. Any altered firmware or OS would require an update signature as captured during a trusted build which could then be used to validate that the update has</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
	<p>to the EMS PCs, any changes to the original deployed system OS will need to be applied and updated into the ES&S System Hardening Document. These updates will then be included in the validation procedure to ensure that all system OS patches have been installed. In regard to ES&S proprietary EMS components, the ES&S Software Validation Procedures will be updated to reflect the new and/or updated components and will be validated through using the hash values supplied by the requisite EAC VSTL.</p> <p>f) As explained above, all OS patches must be reviewed by the appropriate certification authority for the determination of the system testing requirements before the patches can be deployed to the local BOEs. All changed ES&S system components are subject to recertification as determined by NYSBOE.</p>	<p>during a trusted build which could then be used to validate that the update has been applied.</p> <p>f) Updates must go through the certification process as defined by the State of New York.</p>	<p>been applied.</p> <p>f) All changed ES&S system components are subject to re-certification as determined by NYSBOE.</p>
<p>5) Please describe the process of preventing changes to the underlying operating system such as</p> <ul style="list-style-type: none"> a) Code updates b) Configuration modifications c) Loading or unloading DLLs or system 	<p>The hardening process locks the system from administrative privileges for all users other than the system administrator. The system administrator is the only person who may install, modify OS, services, etc.</p>	<p>The DS200 system does not allow access to the internal compact flash card with a keyboard and does not allow booting from an external device. Access to the card is only possible by removing four Torx screws and then taking off the front cover.</p>	<p>A hash check process is thoroughly documented to allow the user to validate that the OS on the device matches the certified one.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>modules</p> <p>d) Turning services on or off</p>		<p>a) A secure digital “signature” or hash of the entire card is made during certification and any modifications are apparent if a subsequent check of the signature does not match.</p> <p>b) OS configuration settings are held in files that are covered under the secure signature generated during certification.</p> <p>c) See answer for a) and b).</p> <p>d) Services are turned on and off using files that would change and any changes would appear as a mismatched signature/hash value.</p>	

Data Security

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>1) What is the data structure that is used for the various components of election data? Detail the vendor, version, etc.</p>	<p>The ElectionWare application uses PostgreSQL 8.3. PostgreSQL is an object-relational database system that has the features of traditional commercial database systems with enhancements to be found in next-generation DBMS systems.</p> <p>http://www.postgresql.org/docs/faqs.FAQ.html</p>	<p>Please refer to Appendix 1 xml schema (xsd files) definitions. These files are named Ballot.xsd, BStylePaper.xsd, Business.xsd, Election.xsd, PollPlace.xsd, and PollPlaceCollection.xsd.</p>	<p>The compact flash card data consists of XML files and associated TXT files for the basic election definition information. In addition, it uses audio and graphic files for display and audio presentation of the ballot information to the user.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>2) What types of access controls are in place to assure security and integrity of the data structure?</p> <p>a) What Authentication mechanisms are used?</p> <p>b) What is the Authorization Matrix? Detail the access to data.</p> <p>c) Do you use role-based access control? Are access permissions based upon defined roles?</p>	<p>Physical access controls are the first access control for all devices, including this device.</p> <p>Windows Access Controls are used to limit access to the system and its applications. Only authorized election workers are permitted access to log in to the EMS PC.</p> <p>The application provides access to the application usage and data by implementing role-based access using database logins and administrator assignments and module access.</p> <p>Encryption is turned on in the database, and access to the database is restricted through the usage of stored procedures. Connectivity is limited to the application.</p> <p>The application uses PostgreSQL 8.3. PostgreSQL is an object-relational database system that has the features of traditional commercial database systems with enhancements to be found in next-generation DBMS systems. PostgreSQL is free and the complete source code is available.”</p> <p>http://www.postgresql.org/docs/faqs.FAQ.html</p>	<p>Physical access controls are the first access control for all devices, including this device.</p> <p>Digital signatures are used to ensure the authenticity/integrity of the data for the DS200.</p> <p>The DS200 is a ballot scanning device. The access to the system for voters is only to insert his/her ballot. The ability to do pollworker functions is controlled by access to the control buttons that are located behind a key-locked door. All other access requires special access codes.</p>	<p>Physical access controls are the first access control for all devices, including this device.</p> <p>All election definition data is stored on the compact flash card. Digital signatures are used to ensure the authenticity/integrity of the data contained on the card. When the card is inserted and the unit is started, the pollworker must enter a password used in the digital signature verification process. Each time the unit is turned, on the file signatures are reverified.</p> <p>The unit requires a physical key to turn it on. The pollworker has no access to the data. Only machine control functions are accessible by the pollworker and these are available in a test position selected using the physical key. The Maintenance menu, accessible from the test position, requires a password for access.</p> <p>Since the unit is activated for voting by inserting an official ballot, access for voting is controlled by ballot issuance. There are no role distinctions associated with the unit.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>3) Are data-specific security counter-measures implemented, e.g. database firewalls, database auditing tools?</p>	<p>http://www.postgresql.org/docs/8.0/static/encryption-options.html</p> <p>PostgreSQL provides many security options, and ES&S is implementing many of them.</p>	<p>Counter measures are physical protection of the device and its ports, as previously described. The DS200 is a standalone device with no other means to access it. The DS200 validates all data it receives for authenticity prior to allowing it to be used on the device. The DS200 digitally signs all data it sends to the EMS so that it can be authenticated prior to using the information.</p>	<p>The AutoMARK has no connection to external devices, communication lines or the Internet. Verification of the election definition files is performed each time the unit is started.</p>
<p>4) In cases where data may be used for development, is data abstracted before being moved into development?</p>	<p>ES&S does not use live data for development.</p> <p>ES&S does use live data for client troubleshooting/assistance. Such data is handled as sensitive data and destroyed after completion of the assistance.</p>		
<p>5) Is encryption utilized?</p> <p>a) What is the implementation approach, i.e. – internal or third-party?</p> <p>b) What algorithms and key sizes are used?</p> <p>c) What is encrypted?</p>	<p>a) & b) ES&S does employ [REDACTED]. The third-party [REDACTED], a NIST CVMP certified software module, is used for this encryption.</p> <p>c) Secure key packages that are exchanged between the EMS PC and the polling locations devices use encryption.</p> <p>Data that is transmitted (if that feature is used) is encrypted.</p>		
<p>6) What controls are in place to ensure data integrity, i.e. how do you make sure that the contents of the data are not being altered directly at the data level?</p>	<p>Digital signatures are used for data exchanged between the EMS PC and the polling location devices to ensure that the data has not been altered.</p>		
<p>7) How are announced security vulnerabilities addressed?</p> <p>a) Is there a formalized risk assessment process to review database vulnerabilities</p>	<p>a) ES&S monitors security alerts on a daily basis for impacts to its voting systems.</p> <p>b) When vulnerabilities are found, ES&S determines proper countermeasures, modifies its systems to include them and notifies its clients of these vulnerabilities and countermeasures.</p> <p>c) ES&S uses technical bulletins to document special procedures that clients should use for technical issue</p>		

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>as they are announced?</p> <p>b) What is the process for testing patches and/or hotfixes identified as required by the risk analysis process?</p> <p>c) Are results of this risk analysis published publicly?</p> <p>d) What is the process for deploying patches to systems as needed?</p> <p>e) Describe the process for validating that appropriate patches and fixes have been deployed</p> <p>f) How is the need for patches and updates addressed through the certification/recertification process?</p>	<p>mitigation, including security issues to which permanent fixes have not yet received certification.</p> <p>d) All changes, including patches to the EMS and embedded firmware in the DS200 and AutoMark, are subject to federal and state certification events.</p> <p>e) Changes to ES&S proprietary EMS components will be validated using an updated set of hashes obtained by the EAC VSTL as part of the trusted build process performed during an EAC or NYSBOE initiated certification event. The ES&S Software Validation Procedures will be updated to reflect the new and/or updated components and will be validated using the hash values supplied by the requisite EAC VSTL.</p> <p>Any change to the DS200 firmware requires approval from a certification authority. During this process, the VSTL generates a signature/hash using a federally approved algorithm. Users can guarantee only approved components are installed by generating a signature and comparing the result to the signature generated during certification.</p> <p>f) All changed ES&S system components are subject to recertification as determined by NYSBOE.</p>		
<p>8) What applications are used to create reports directly from the data? How is security of the reporting applications maintained?</p>	<p>Report generation is handled within the application; as a part of the application, it is secured under the same methods as the rest of the application. Any reports generated outside the application are not part of the certified application.</p>		

Network Security

Currently networking of EMS equipment, pollsite voting systems and disability voting systems is prohibited by NY State Election Law. Please address the following questions in consideration of change of that requirement – i.e. if networking were to be allowed in the future what would be the answers to these questions

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>1) Do any of the major components have physical network connections available? Could physical network connections be installed without detection?</p>	<p>The current ES&S System Hardening procedures of the EMS PC remove the use of all networking protocols.</p> <p>If transmission of election results becomes sanctioned by NYSBOE,</p>	<p>The DS200 does not have a network connection available. It also does not have a modem installed.</p> <p>In systems where ES&S does provide a modem, the DS200</p>	<p>The ES&S AutoMARK does not have any network connectivity.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
	<p>a separate data transmission server may be used as a method for receiving election night unofficial polling location results from either regional collection centers or directly from the polling places. All such transmission is encrypted, as previously described. Once received, these results are validated for authenticity using the digital signatures they contain, prior to allowing their utilization.</p>	<p>features for activating and using the modem require pollworker access to the controls behind the key-lock door and special access codes. The modem can not be activated until polling has closed.</p> <p>Optionally, an external PC can be used at the polling location or regional collection point to establish a secure network connection the central location data transmission reception server.</p>	
<p>2) If any of the above received a “YES”, please describe in detail countermeasures used to ensure that only authorized connectivity can occur.</p>	<p>Secure CoreFTP will be used to authenticate all connection points to the data transmission server. Additionally, all transmitted results data will be encrypted and digitally signed. The EMS application validates all data file signatures before applying the data to the EMS results database.</p>	<p>In systems where ES&S does provide a modem, the DS200 is capable of encrypting all data sent across the connection with a federally approved AES algorithm.</p>	<p>The ES&S AutoMARK does not have any network connectivity.</p>
<p>3) Do any of the major components have the capability for connection via wireless connectivity, e.g. WiFi, Bluetooth, Cellular technology (AMPS, D-AMPS, CDMA2000, GSM, GPRS, EV-DO, and UMTS)? If so, which and why?</p>	<p>The EMS PCs will be hardened according to the ES&S System Hardening procedures, which will initially remove all such connectivity options. Should transmission of results data be approved, only the data transmission server and requisite sending device will be</p>	<p>The DS200 does not possess wireless capability.</p>	<p>The ES&S AutoMARK does not have any network connectivity, wireless or otherwise.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
	enabled to connect to remote devices. All other EMS PCs will remain isolated from all external connections.		
4) If any of the above received a "YES", please describe in detail countermeasures used to ensure that wireless data transmissions will be secure from breaches of confidentiality or integrity.	All transmitted data, whether using wired or wireless protocols, is encrypted and digitally signed.	All transmitted data, whether using wired or wireless protocols, is encrypted and digitally signed.	The ES&S AutoMARK does not have any network connectivity.
5) What kinds of network security does the system provide to support networking capabilities that may be added later?	The EMS will be deployed on standard Windows based Servers and PCs and will use standard networking protocols. This deployment allows NYC to select from a wide array of third party network security tools to provide the level of security deemed necessary by NYC.	The DS200 is capable of signing and encrypting all data with FIPS (Federal Information Processing Standard) approved algorithms and programs.	The ES&S AutoMARK does not have any network connectivity. There is no functional advantage for the AutoMARK to have network attachment capability.

Application Development Security

Control Definition	EMS	Pollsite Voting System	Disability Voting System
1) What development platform(s) were utilized for each major component?	<p>The EMS is developed as 32-bit Windows applications.</p> <p>Microsoft Visual Studio 6.0 Microsoft Visual Studio 2005</p> <p>Sun JDK 6 (Swing)</p> <p>Liant RM/COBOL with WOW Extensions 11.01</p> <p>The underlying source code</p>	<p>The DS200 firmware is developed using a standard Linux GNU Open Source tool chain.</p> <p>The compiler is the GNU Compiler Collection (GCC) V 4.0.3.</p> <p>The user Interface component is written in Java using the Java 6 Standard Edition V 6.0.0.3.</p>	<p>Software required for compiling and loading firmware/software for the ES&S AutoMARK VAT includes:</p> <p>Microsoft Embedded Visual C++ 4.0 Service Pack 4.</p> <p>Microsoft Visual Studio .NET 2003 Service Pack 2.</p> <p>Keil Software µVision2, C</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
	<p>consists of C, Visual C++, JAVA and OO Cobol.</p>	<p>The Encryption Library is from RSA version BSafe Crypto CME 2.0.0.</p> <p>The Power Management Board is developed using the IAR Embedded Workbench IDE V 4.6 for W32 that uses the IAR C/C++ Compiler for MSP430 V 3.40.1.9</p> <p>The Scanner control board is developed using the uVision3 IDE V3.51, C Compiler V 8.08, Assembler V8.08d, Linker/Locator V 6.05, Librarian V4.24, Hex Converter V 2.6.</p> <p>C/C++ language XML parsing code is generated using CodeSynthesis XSD version 3.1.0 from Code Synthesis Tools CC..</p>	<p>compiler Version 2.40.</p> <p>Texas Instruments Code Composer Studio. Version 2.0.</p> <p>Cosmic Compiler V 4.1H</p> <p>Prog08sz Programmer for v 2.05.</p> <p>Atmel Flip v2.4.6.</p> <p>Atmel MCU ISP Software V1.0.</p> <p>Microsoft Windows CE With Platform Builder Version 5.0.</p>
<p>2) Is source code available for public review?</p>	<p>Because the source code is key to the continued operation of ES&S' business and constitutes a trade secret as well as for the security of ES&S' voting systems, ES&S does not make its voting system source code available for the public to review.</p> <p>As a standard practice, ES&S maintains in escrow with Iron Mountain Intellectual Property Management, Inc., a copy of all program source code developed and used for our proprietary software and firmware, as well as any changes, modifications or updates to the source code. If the City requires the escrow to be with another party, it shall pay the additional cost associated therewith. Should ES&S cease operations and become unable to maintain and support our proprietary software and firmware while under an obligation to do so, the City shall have the right to obtain the source code to the extent necessary to enable the City to use ES&S' proprietary software and firmware in accordance with the terms of the final contract agreed upon by the parties. As the source code to ES&S' voting system software and firmware is ES&S' proprietary intellectual property which constitutes a trade secret, ES&S cannot otherwise agree to a release of the source code to the City. The source code shall, at all times, remain the property of ES&S and may not otherwise be used by the City.</p>		
<p>3) What is your internal process for testing</p>	<p>ES&S has embraced the Agile development methodology. As part of this methodology, short development</p>		

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>applications? Are the results of internal testing publicly available?</p>	<p>cycles are completed and the resultant code is promoted to the ES&S Quality Assurance Department (QA). Unit testing is performed by the Development Staff and then delivered to the ES&S QA Department at the end of each iteration.</p> <p>After a product version is delivered to QA, the enhancements and bug fixes included in the release are assigned to the individual QA Analyst responsible for that product. The analyst utilizes standardized test case documentation and employs multiple datasets to verify each enhancement has been implemented appropriately. Regression and integration testing is also performed at regular intervals. Test case and other test documentation is considered proprietary information and is not publicly available.</p>		
<p>a) Do you submit applications for independent test (in addition to state and federal required reviews)?</p> <p>b) Are the results of the review publicly available?</p> <p>c) What is the process for addressing vulnerabilities and risks identified during independent testing?</p>	<p>a) ES&S welcomes thorough examinations of important elements of the electoral process. For many years, we have participated in extensive testing and review conducted by independent testing authorities, state and local election officials, and other third parties. Time after time, ES&S has worked with those conducting such reviews to provide needed information and access to voting system and technology. We believe independent, rigorous and fair evaluations of voting systems help to strengthen the performance of voting technology and those who produce it.</p> <p>b) Results and conclusions from these independent tests are usually made public. Items that deal with system security are redacted from these reports.</p> <p>c) Vulnerabilities and risks identified during these independent testing events are assessed by ES&S. Those that are found credible are addressed in future development plans.</p>		
<p>4) What is the process for patching bugs or security vulnerabilities in the applications?</p> <p>a) What is the process for testing patches required by the risk analysis process?</p> <p>b) Are results of this risk analysis published publicly?</p> <p>c) What is the process for deploying patches to systems as needed?</p> <p>d) Describe the process for validating that appropriate patches and fixes have been deployed</p> <p>e) How is the need for patches and updates addressed through the certification/</p>	<p>ES&S, as is all election system vendors, is required to perform federal, and in most cases, state certification testing of all product changes, both software and hardware.</p> <p>a) Product improvements and patches are scheduled and scoped into product releases. These changes go through the normal ES&S QA testing process.</p> <p>b) System issues are routinely distributed to the ES&S customer base via a Technical Bulletin process. The items identified in the Technical Bulletins can originate from a number of sources – Independent testing, current customers, ES&S internal use, ES&S QA testing.</p> <p>c) As stated above, each and every change to the voting system is subjected to federal and state certifications before they can be released.</p> <p>d) ES&S has developed a software validation process that verifies hash codes of all ES&S developed system components. The hash codes are created by and made available to the local jurisdictions by the EAC-approved VSTL as a byproduct of the VSTL trusted build process.</p> <p>e) See c) above.</p>		

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>recertification process?</p>			
<p>5) Provide a list of known bugs and vulnerabilities in the current released version and provide an indication of what the process and the time frame is to address them.</p>	<p>An integral part of the ongoing State of New York Lot 1 Certification project is the execution of all ES&S system components through a series of test cases. These test cases, first developed by the testing authority and then reviewed and amended by NYSBOE and NSYTEC, are designed to test all parts of the proposed voting system. Test cases are developed and conducted to test all requirements of the 2005 VVSG. The list of known vulnerabilities is listed as documented on the EAC website, www.eac.gov. Any identified discrepancies documented by the testing authority as these test cases are exercised against the proposed ES&S voting system, including the ES&S EMS, DS200 digital optical scanner and AutoMARK ballot marking device, are addressed by ES&S in subsequent builds of the affected voting system component, reviewed at the source code level, and then retested through the respective test cases. Successful completion of the State of New York Lot 1 Certification project ensures that all of these discrepancies have been resolved by ES&S and retested by the testing authority.</p>		
<p>6) What is the SDLC methodology used in the development of each major component?</p>	<p>ES&S uses the Agile development methodology. Part of the ES&S Technical Package included in all certification events is the ES&S Software Development Methodology document.</p>		
<p>7) Describe the process of moving new applications or versions from development to QA, to staging and into production.</p>	<p>Regular release planning sessions are held to determine the scope of a given release. Once the development team has completed its goals for the current iteration – or short development cycle – a development build of each product is prepared by the Configuration Management (CM) department and staged at a central location for the Quality Assurance department to evaluate. Each enhancement or bug fix in scope for the release is reviewed, and regression testing is likely to be performed as well.</p> <p>Once all development iterations for a release have been completed and tested, CM transfers the release, using a secure FTP site, to the Voting System Test Laboratory (VSTL). The VSTL and CM perform a trusted build of the release. With assistance from the ES&S Certification department, the VSTL then performs the functional testing required for the release.</p> <p>Upon completion of the testing and with NYS Board of Election approval of all test results, the release is made available for production. The VSTL continues to maintain the chain of custody of the production release and is responsible for the distribution and/or validation of the release as received by the customer.</p>		
<p>8) Does the SDLC have checkpoints built into the process to ensure that no bugs or vulnerabilities have been introduced prior to deployment into production?</p>	<p>The ES&S Quality Assurance department verifies that no bugs or vulnerabilities have been introduced through the use of regression and integration testing methods. Regression testing involves following documented processes to verify that traditional or previous features of the system have not been affected by new development. With regards to integration testing, the Quality Assurance department utilizes a team methodology to verify end-to-end processing accuracy of multiple election datasets. Both regression and integration testing are performed at regular intervals during the development process.</p>		

Control Definition	EMS	Pollsite Voting System	Disability Voting System
9) What checks and balances are in place to ensure that application code does not vary from “approved” versions?	ES&S has developed a Software Validation Process that verifies hash codes of all ES&S-developed system components. The hash codes are created by and made available to the local jurisdictions by the EAC approved VSTL as a byproduct of the VSTL trusted build process		

Application Functional Security

Control Definition	EMS	Pollsite Voting System	Disability Voting System
1) What are the formats of vote results data, for the pollsite voting system and in the EMS, i.e. what is the storage mechanism, what are the logical structure types of the data?	The ES&S EMS processes election results from a USB memory stick removed from each DS200 as part of the poll closing process. The structure of the individual files captured by the DS200 onto the USB memory stick is described in the Pollsite Voting System response for this same question. The PollPlaceCollection.xml file is read from each USB memory stick to update the results for each election district into a jurisdiction-wide results database.	The DS200 saves an xml ballot record (schema available in Appendix 1) containing voter marks every time a ballot is cast. These records are saved to the external USB memory stick locked under the front top door of the unit. As an optional, selectable process, the unit can save a viewable image of the front and back of the ballot as scanned. These images are saved in .pmb (portable bitmap graphic) format and are also stored on the portable USB drive. When a user closes the unit, the DS200 creates a PollPlaceCollection.xml file (schema available in Appendix 1) that contains accumulated totals as derived from the individual ballot records.	The ES&S AutoMARK is a ballot marking device and does not record vote results.
2) What integrity checks are built-in to ensure the votes cast are the votes recorded?	Correct processing of marked ballots is the responsibility of the DS200 firmware as described in the Pollsite Voting System response for	The initial mark gathering/ interpretation routines employ a patented IMR (Intelligent Mark Recognition) system designed	The ES&S AutoMARK is a ballot marking device and does not record vote results.

Control Definition	EMS	Pollsite Voting System	Disability Voting System
	<p>this question. The ES&S EMS processes the aggregated vote totals for each office and candidate from the PollPlaceCollection.xml written onto each USB memory stick at poll close time. In addition to the validation of all digitally signed files on each USB memory stick, the ES&S EMS performs integrity checks on all contest and candidate vote totals before updating of election results occurs to the results database. These integrity checks include: 1) The sum of all candidate votes plus overvotes and undervotes in the contest must equal the total ballots cast in each election district (multiple vote-for offices taken into consideration in this check.) 2) The number of candidate counters expected to be received from each election district matches the counters received from each DS200. 3) The user may set thresholds relevant to the registered voters in each election district as a means to validate ballots cast versus registered voters in a given election.</p>	<p>and tested to very accurately detect all kinds of marks. Accuracy is carefully tested during certification.</p> <p>When a voter inserts a ballot, the system checks for proper marks and presents an information screen displaying over/under votes if they exist.</p> <p>Every ballot record is saved with a unique digital signature and file name for later validation.</p>	
<p>3) What mechanism is in place to ensure that there is a clear one-to-one correspondence between ballots cast and all electronic records?</p>	<p>All voter records are saved in files with names derived from a unique/random 64-bit number. Each record type associated with the same ballot carries a common portion of the file name such that they can be matched.</p>		<p>The ES&S AutoMARK is a ballot marking device and does not record vote results.</p>
<p>4) Where are the aggregated vote totals stored (please discuss physical and logical</p>	<p>The ES&S EMS stores aggregated vote totals at both the election</p>	<p>Aggregated vote totals are generated when the device is</p>	<p>The ES&S AutoMARK is a ballot marking device and does not record</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
mechanisms)	district and jurisdiction level in the election-specific results database built from each unique election definition.	closed and the file holding the totals is signed and stored on the removable USB memory stick.	vote results.
5) How is access to the EMS (central vote tally) controlled, i.e. what types of access control prevents access to the underlying data?	<p>The EMS runs on a PC under the Windows XP Operating System. The OS is resident on the PC hard drive.</p> <p>a) The protections for this OS include lockdown of the BIOS and maintaining the PC in a physically controlled location. Other controls to protect the PC include hardening of the Windows OS so that only authorized users can log in and so that only authorized system administrators can perform administrative functions.</p> <p>b) Vote results are stored on the EMS PC on its hard drive, which is protected as described above.</p> <p>c) Election information and ballot definitions on the EMS PC are stored on its hard drive, which is protected as described above</p>	The DS200 is not part of the EMS.	The ES&S AutoMARK is a ballot marking device and does not record vote results.
6) What controls prevent tampering with vote results at pollsites?	Not applicable to the EMS.	During operation while the polls are open, the USB memory stick is kept behind a sealed and locked door. All ballot and collection data is signed with unique digital signatures using keys deployed from a separate USB memory stick.	The ES&S AutoMARK is a ballot marking device and does not record vote results.

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>7) Describe the canvass process</p> <p>a) Where are the physical paper ballots stored after they are cast at the pollsite?</p> <p>b) What is the proscribed method for conducting an audit?</p>	<p>a) Not applicable to the EMS</p> <p>b) An audit between the poll site election results tapes produced by each DS200 at poll close should be audited against election district results reports printed from the EMS after the processing of all USB memory sticks.</p> <p>The public counter on each DS200 should be audited against the count of registered voters that vote at each poll site.</p>	<p>a) Cast ballots remain in the locked ballot box bin until removed by the election official for official canvass.</p> <p>b) On Election Day the initial audit is performed by comparing the poll worker records with the machine reports.</p> <p>Because the DS200 is a paper ballot pollsite counter, subsequent audits are performed post-Election Day by rescanning the ballots from a particular machine/poll place and comparing the outcome to Election Day results.</p>	<p>The ES&S AutoMARK is a ballot marking device and does not record vote results requiring canvass.</p>
<p>8) What is the mechanism and process for moving vote tallies and associated data from the pollsite voting systems to the EMS system?</p>	<p>At poll close, each DS200 creates a Poll Place Collection Data XML file, digitally signs it and stores it on the USB memory stick, along with all other DS200-specific ballot and report data. The USB memory tick is then transported to the site of the ES&S EMS reporting system. There, the USB memory stickss are read into the election-specific results database created by the ES&S EMS. The results files are authenticated and validated through the use of a public/private key pair and then updated into the jurisdiction-wide results database.</p>	<p>At poll close, the DS200 creates a Poll Place Collection Data file, signs it and stores it on the USB memory stick, along with all other ballot and report data. The USB memory stick is then transported to the site of the EMS reporting system. The files are authenticated and validated through the use of a public/private key pair.</p>	<p>The ES&S AutoMARK is a ballot marking device and does not record vote results.</p>
<p>9) What controls are in place to assure that the results (memory card, CD etc.) which leave</p>	<p>The DS200 employs an FIPS certified public/private key pair</p>	<p>The DS200 employs a FIPS certified public/private key pair</p>	<p>The ES&S AutoMARK is a ballot marking device and does not record</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
the pollsite are the same as those entered into the EMS	system that allows detection of any unauthorized changes to any record generated on the machine. The ES&S EMS system authenticates all digital signatures before using any results data from each USB memory stick. Each DS200 uniquely digitally signs all files written to each USB memory stick.	system that allows detection of any unauthorized changes to any record generated on the machine.	or store vote results.
10) For disability voting, what controls are built-in to ensure that the information presented to the voter matches the ballot information, i.e. a visually impaired user is read the list of candidates – how do we know that the read list matches the printed list in order and content?	The ES&S EMS contains an AutoMARK emulator function that allows both the visual display and audio presentation of each ballot style to be verified by the user at the time of election definition before the election definition is finalized and loaded onto each AutoMARK.	Not applicable. Disability voting is accomplished on the ES&S AutoMARK BMD.	Each election data element, in both visual and audio forms, is linked via the database used by ElectionWare. The same database is used in the physical creation of the ballot artwork. ElectionWare has an AutoMARK emulator function that allows both the visual display and audio presentation to be verified. The AutoMARK itself has a test print function that verifies the voted candidate selects the proper candidate on the physical ballot.
11) What types of integrity controls are in place to assure that results have not been tampered with at the pollsite?	The EMS validates the digital signatures on all results files received from the polling location to ensure they have not been tampered with.	The media holding the ballot records are kept behind a sealed and locked door on the DS200 during voting hours. As mentioned in item 9, all data is signed public/private key pairs.	The ES&S AutoMARK is a ballot marking device and does not record vote results.
12) What types of integrity controls are in place to assure that results have not been tampered with at the EMS location?	Windows access controls are used to limit access to the system and its applications. Only authorized election workers are permitted access to log in to the EMS PC.	The DS200 is not part of the EMS system, but all data held on memory sticks from the machine is signed with a secure key pair.	The ES&S AutoMARK is a ballot marking device and does not record vote results.

Control Definition	EMS	Pollsite Voting System	Disability Voting System
	<p>The ES&S EMS contains detailed audit logs capturing all programmatic and manual updates to election results.</p> <p>The recommended auditing process validates vote totals stored in the results database back to the DS200 results tapes. This validates the contents of the results at the EMS location.</p>		
<p>13) What types of access controls are in place to assure security and integrity of the application and associated modules?</p> <p>a) What Authentication mechanisms are used?</p> <p>b) What is the Authorization Matrix? Detail the access to data.</p> <p>a) Do you use role-based access control? Are access permissions based upon defined roles?</p>	<p>Physical access controls are the first access control for all devices, including this device.</p> <p>Windows access controls are used to limit access to the system and its applications. Only authorized election workers are permitted access to login to the EMS PC.</p> <p>The application provides access to the application usage and data by implementing role-based access using database logins and administrator assignments and module access.</p> <p>Encryption is turned on in the database, and access to the database is restricted through the usage of stored procedures. Connectivity to the application is limited.</p> <p>The application uses PostgreSQL 8.3. PostgreSQL is an object-relational database system that has</p>	<p>Physical access controls are the first access control for all devices, including this device.</p> <p>Digital signatures are used to ensure the authenticity/integrity of the data for the DS200.</p> <p>The DS200 is a ballot scanning device. The access to the system for voters is only to insert his/her ballot. The ability to do pollworker functions is controlled by access to the control buttons that are located behind a key-locked door. All other access requires special access codes.</p>	<p>Physical access controls are the first access control for all devices, including this device.</p> <p>All election definition data is stored on the compact flash card. Digital signatures are used to ensure the authenticity/integrity of the data contained on the card. When the card is inserted and the unit is started, the pollworker must enter a password used in the digital signature verification process. Each time the unit is turned on the file signatures are reverified.</p> <p>The unit requires a physical key to turn it on. The pollworker has no access to the data. Only machine control functions are accessible by the pollworker and these are available in a test position set selected using the physical key. The Maintenance menu, accessible from the test position, requires a password for access.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
	<p>the features of traditional commercial database systems with enhancements to be found in next-generation DBMS systems. PostgreSQL is free and the complete source code is available.</p> <p>http://www.postgresql.org/docs/faqs.FAQ.html</p>		<p>Since the unit is activated for voting by inserting an official ballot, access for voting is controlled by ballot issuance. There are no role distinctions associated with the unit.</p>
<p>14) What is the end-to-end chain-of-custody for the software and firmware in each component?</p>	<p>As part of the State of New York and all federal EAC certification events, the state and/or federally approved VSTL performs trusted builds of all software and firmware components. As part of the trusted build process, the VSTL creates hash codes for each system component. These hash codes are created by and made available to the local jurisdictions by the EAC approved VSTL as a byproduct of the VSTL trusted build process. ES&S has developed a software validation process that allows each installed user to verify the VSTL generated and provided hash codes of all ES&S developed system components. The software validation procedure may be performed at any time to ensure that the installed system exactly matches the certified system.</p>	<p>The chain of custody is dependent upon the requirements of a particular jurisdiction. Typically, the VSTL performs a trusted build of the software and firmware and then generates a digital signature and /or hash value for validation. Individual jurisdictions can obtain the software and firmware from the VSTL or other trusted source and validate the components using the published hash values and/or signatures.</p>	
<p>15) How do the Pollsite Voting System and the EMS prevent the introduction of results from other jurisdictions' election definitions, ballots, and results?</p>	<p>The jurisdiction-wide, election-specific key programmatically generated by the ES&S EMS for each election is randomly generated and therefore unique to</p>	<p>The jurisdiction-wide, election-specific key programmatically generated by the ES&S EMS for each election is randomly generated and therefore unique</p>	<p>The AutoMARK is a ballot marking device. There are no results created or stored in the unit.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
	<p>a given election event. Elections generated for other jurisdictions and/or other elections will be created using a differently key, also randomly generated, that will fail the authentication and validation tests performed by the DS200 and EMS.</p>	<p>to a given election event. Elections generated for other jurisdictions and/or other elections will be created using a differently key, also randomly generated, that will fail the authentication and validation tests performed by the DS200.</p>	

Miscellaneous

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>1) What is the process for addressing potential breaches of system security, i.e. incident response – possible scenarios would be:</p> <ul style="list-style-type: none"> a) A malicious attacker gains access to your source code b) An attacker gains access to aggregated raw election data either at a polling location or at the EMS location 	<p>Each compromise would be evaluated for any potential impact and the appropriate action and/or countermeasure would be enacted. ES&S security specialists would be consulted, and the appropriate level of management and customer communications would be involved. In the specific example scenarios.</p> <ul style="list-style-type: none"> a) Access to the source code of our system would not compromise the system. ES&S maintains daily backups of our source code libraries for restoration if necessary. Such disclosure would make it possible for a malicious attacker to search for previously unknown vulnerabilities, but the controls in place provide security that the systems used are the authentic ones. Also, such a disclosure would compromise our corporate intellectual property. b) Raw election data has nothing that can compromise the official results. All data processed for the official results is automatically validated (using the digital signatures) to ensure its authenticity. An attempt to introduce counterfeit results would be detected and prevented. Additionally, keep in mind that audit and canvassing processes – which would involve the originally voted ballots, paper tapes from the tabulators, and central database records – would identify any malicious activity by an attacker. 		
<p>2) What is the process for analyzing identified risks and developing countermeasures or mitigating controls to identified risks and vulnerabilities?</p>	<p>This is part of our software development process. Security of the application is incorporated in the work.</p>		
<p>3) What tools do the systems provide to support re-canvassing and statistically validating election results?</p>	<p>The ES&S EMS includes embedded integrity checks to ensure that only valid aggregated</p>	<p>Recanvassing and statistically validating election results can be accomplished by rescanning the</p>	<p>The ES&S AutoMARK is a ballot marking device and does not record vote results.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
	<p>vote totals are introduced into the results database. It is also usual and customary practice to conduct a discovery recount after each election. This statistical sampling involves the rescanning and retabulation of voted ballots in a statistically sound percentage of the total jurisdiction. Should the discovery recount identify a variance outside the range of tolerance, a larger statistical sampling is performed. The results of the second sampling then dictate if a total recount is warranted.</p>	<p>ballots.</p>	