

**BOE in NYC
RFI for Voting System
Addendum # 2
Additional Security Questions
for**

Sequoia Voting Systems & Democracy Suite

January 19, 2009

Table of Contents

Physical Security	2
Operating System Security	3
Data Security.....	5
Network Security	7
Application Development Security.....	8
Application Functional Security	10
Miscellaneous	13

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> <p>a) Storage containing operating system (Technology, Interface Form factor, location, physical segregation, etc)</p> <p>b) Storage of vote results (Technology, Interface Form factor, location, physical segregation, etc)</p> <p>c) Storage of election information and ballot definitions.</p> <p>d) Printer for results and status messages</p>	<p>The EMS system runs off commodity PC server hardware enclosed in a standard rack mount chassis. It uses standard SATA hard drives to hold both election coding and results data.</p> <p>All Data is stored securely inside Microsoft SQL 2005 Server and data produced (e.g. election files and ballots) is encrypted and/or signed using industry standard algorithms.</p>	<p>The poll site voting system uses key locks (which are randomized among the manufactured units) for physical security along with tamper-proof seals.</p> <p>Results are held encrypted on CF cards inside the tabulator (behind locks and seals).</p> <p>The tabulator printer is secured with locks and/or seals.</p>	<p>The poll site voting system uses key locks (which are randomized among the manufactured units) for physical security along with tamper-proof seals.</p> <p>Results are held encrypted on CF cards inside the tabulator (behind locks and seals).</p> <p>The tabulator printer is secured with locks and/or seals.</p> <p>The accessibility printer and hardware is sealed using security screws and security seals.</p>
<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>The complete system is protected with RAID 10 redundant storage technology. Tabulation data can be copied onto removable media for additional backup purposes.</p>	<p>The system has two cards, one primary and one secondary should the primary fail or become unavailable.</p>	<p>The system has three cards, one primary and one secondary results card should the primary fail or become unavailable. A third card is used as the O/S for the accessibility display.</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>The server system can have temper-proof seals attached to the case where it could potentially be opened for modification.</p>	<p>The firmware is hashed at the VSTL. This hash can be extracted at any time for verification.</p>	<p>The firmware is hashed at the VSTL. This hash can be extracted at any time for verification.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
4) Please list all ports on the unit with descriptions of form factors, communication protocols and purpose	RJ45 (closed network), PS2 (keyboard and mouse), USB (security key and memory cards)	RJ45 (custom wired for ATI), 3.5mm audio headset jack, RS232 serial port (read only)	RJ45 (custom wired for ATI)
5) What capability is in place to secure ports from access by unauthorized connections, e.g. connecting a portable computing unit to the ports	You can apply tamper-proof seals to the ports when they are not being legitimately used.	The ports are not capable or configured to accept such a device.	The ports are not capable or configured to accept such a device.
6) Are all modular and removable components (such as printers and memory modules) serialized to track system assemblies and sub assemblies?	Yes, all components are individually serialized by there respective manufacturers.	Yes, all components are individually serialized.	Yes, all components are individually serialized.

Operating System Security

Control Definition	EMS	Pollsite Voting System	Disability Voting System
1) What is the underlying operating system? Detail the manufacturer, version, build and all relevant updates and patches.	Microsoft Windows XP Professional SP2 Microsoft Windows Server 2003 Standard and/or Enterprise SP2	ucLinux embedded Linux operating system	ucLinux embedded Linux operating system (tabulator) and Gentoo Linux 2.0
2) Is there a standardized process for hardening of operating system components prior to delivery to the board of elections? a) What is the process for hardening the operating systems? b) Is the process available for public review? c) What is the process for validating that the process is adhered to?	Our system includes an application (EMS DCM) that hardens the OS before the rest of the EMS system is installed. This ensures the system meets appropriate security requirements as all other EMS applications will not operate if this is not completed successfully.	OS consists of extremely limited set of binaries that are just enough to run the application with minimal user access and without communication protocols.	OS consists of extremely limited set of binaries that are just enough to run the application with minimal user access and without communication protocols.

Control Definition	EMS	Pollsite Voting System	Disability Voting System
3) What is the mechanism and process used to install the operating system?	The operating system is installed using either CD or DVD media.	The firmware (operating system) is installed via CF card using a secure firmware installation security key.	The firmware (operating system) is installed via CF card using a secure firmware installation security key.
4) How are announced security vulnerabilities addressed? <ul style="list-style-type: none"> a) Is there a formalized risk assessment process to review OS vulnerabilities as they are announced? b) What is the process for testing patches and/or hotfixes identified as required by the risk analysis process? c) Are results of this risk analysis published publicly? d) What is the process for deploying patches to systems as needed? e) Describe the process for validating that appropriate patches and fixes have been deployed f) How is the need for patches and updates addressed through the certification/recertification process? 	Microsoft provides periodic updates via their website. Machines are updated to most recent Service Packs when made available by Microsoft. <ul style="list-style-type: none"> a) This can be preformed independently by the end-user. b) The "Election Readiness Test" is preformed after any single or group of patches are installed. c) NA d) Manufacturer provided service pack CD or binary e) Automatically indicated by O/S f) Unknown at this time 	Operating system version is frozen.	Operating system version is frozen.
5) Please describe the process of preventing changes to the underlying operating system such as <ul style="list-style-type: none"> a) Code updates b) Configuration modifications c) Loading or unloading DLLs or system modules d) Turning services on or off 	Code updates would result in the application breaking the hash matching the one supplied by the VSTL.	Code updates result in changes to the hash which would invalidate the hash checks preformed before each election. There is no method to make configuration changes, loading/unloading of system models or turning on/off services while the system is in operation.	Code updates result in changes to the hash which would invalidate the hash checks preformed before each election. There is no method to make configuration changes, loading/unloading of system models or turning on/off services while the system is in operation.

Data Security

Control Definition	EMS	Pollsite Voting System	Disability Voting System
1) What is the data structure that is used for the various components of election data? Detail the vendor, version, etc.	The data structure is held within a Microsoft SQL 2005 database.	The data structure is proprietary binary format.	The data structure is proprietary binary format.
2) What types of access controls are in place to assure security and integrity of the data structure? a) What Authentication mechanisms are used? b) What is the Authorization Matrix? Detail the access to data. c) Do you use role-based access control? Are access permissions based upon defined roles?	Microsoft SQL 2005 includes various levels of security built-in including but not limited to encrypted passwords, role-based access control, and full login and query auditing.	The data structure is encrypted and the tabulator has full audit capabilities. a) 'iButton' security key allows for poll worker/administrator to decrypt election files and check hashes for validity b) No authorization matrix exists c) No	The data structure is encrypted and the tabulator has full audit capabilities. a) 'iButton' security key allows for poll worker/administrator to decrypt election files and check hashes for validity b) No authorization matrix exists c) No
3) Are data-specific security counter-measures implemented, e.g. database firewalls, database auditing tools?	The EMS application has auditing tools for the application and database levels.	The poll site voting system has an audit module built-in.	The poll site voting system has an audit module built-in.
4) In cases where data may be used for development, is data abstracted before being moved into development?	NA	NA	NA
5) Is encryption utilized? a) What is the implementation approach, i.e. – internal or third-party? b) What algorithms and key sizes are used? c) What is encrypted?	Yes, encryption is utilized a) mixture standard of symmetric and asymmetric encryption and signing algorithms b) Asymmetric encryption: [REDACTED] hashing, Asymmetric encryption [REDACTED]	Yes, encryption is utilized a) mixture standard of symmetric and asymmetric encryption and signing algorithms b) Asymmetric encryption: [REDACTED] Asymmetric encryption [REDACTED]	Yes, encryption is utilized a) mixture standard of symmetric and asymmetric encryption and signing algorithms b) Asymmetric encryption: [REDACTED] hashing, Asymmetric encryption [REDACTED]

Control Definition	EMS	Pollsite Voting System	Disability Voting System
	c) Election files and results are encrypted and signed.	c) Election files and results are encrypted and signed.	c) Election files and results are encrypted and signed.
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?	The official ballots, audio files, visual files, and XML files used for the tabulation system are [REDACTED] encrypted.	Modification of the data on the poll site tabulator will result it from either not functioning (warning presented) or failing hash checks.	Modification of the data on the poll site tabulator will result it from either not functioning (warning presented) or failing hash checks.
7) How are announced security vulnerabilities addressed? a) Is there a formalized risk assessment process to review database vulnerabilities as they are announced? b) What is the process for testing patches and/or hotfixes identified as required by the risk analysis process? c) Are results of this risk analysis published publicly? d) What is the process for deploying patches to systems as needed? e) Describe the process for validating that appropriate patches and fixes have been deployed f) How is the need for patches and updates addressed through the certification/recertification process?	Complete system reinstall. A) No B) NA C) No D) NA E) NA F) NA	Complete system reinstall. A) No B) NA C) No D) NA E) NA F) NA	Complete system reinstall. A) No B) NA C) No D) NA E) NA F) NA
8) What applications are used to create reports directly from the data? How is security of the reporting applications maintained?	Reports in the system are generated from within the certified application. The security of this data is as good as the certification process it went under.	Reports in the system are generated from within the certified application or form the main EMS system once results are returned to the central site.	Reports in the system are generated from within the certified application or form the main EMS system once results are returned to the central site.

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
1) Do any of the major components have physical network connections available? Could physical network connections be installed without detection?	Yes. The EMS system contains network ports (RJ45) that are used with the closed-network configuration.	No	Yes. An RJ45 jack is integrated into the motherboard.
2) If any of the above received a “YES”, please describe in detail countermeasures used to ensure that only authorized connectivity can occur.	Additional network connections could not be installed without the operating system detecting them.	NA	The RJ45 jack is inaccessible without bypassing seals and security screws. The RJ45 device is also disabled at boot. Even if the RJ45 port is accessed, there is no access to election/results files from the accessibly portion of device.
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?	No	No	No
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.	NA	NA	NA
5) What kinds of network security does the system provide to support networking capabilities that may be added later?	Windows firewall, NAT and other standard windows-based security protocols and features.	Network capabilities are not allowed under current regulations.	Network capabilities are not allowed under current regulations.

Application Development Security

Control Definition	EMS	Pollsite Voting System	Disability Voting System
1) What development platform(s) were utilized for each major component?	Visual Studio 2005 and .NET 2.0	Linux IDE	Linux IDE
2) Is source code available for public review?	No	No	No
3) What is your internal process for testing applications? Are the results of internal testing publicly available?	Engineering Testing → Development QA → Company QA → Product testers The test results are not publicly available.	Engineering Testing → Development QA → Company QA → Product testers The test results are not publicly available.	Engineering Testing → Development QA → Company QA → Product testers The test results are not publicly available.
a) Do you submit applications for independent test (in addition to state and federal required reviews)? b) Are the results of the review publicly available? c) What is the process for addressing vulnerabilities and risks identified during independent testing?	a) None besides state/federal b) NA c) NA	a) None besides state/federal b) NA c) NA	a) None besides state/federal b) NA c) NA
4) What is the process for patching bugs or security vulnerabilities in the applications? a) What is the process for testing patches required by the risk analysis process? b) Are results of this risk analysis published publicly? c) What is the process for deploying patches to systems as needed? d) Describe the process for validating that appropriate patches and fixes have been deployed	All issues are entered into a production-quality bug tracking system. Items are assigned to developers, for correction, and then tested by QA to ensure proper resolution of issues. a) Patches are not used b) No / NA c) Patches are not used d) NA e) NA	All issues are entered into a production-quality bug tracking system. Items are assigned to developers, for correction, and then tested by QA to ensure proper resolution of issues. a) Patches are not used b) No / NA c) Patches are not used d) NA e) NA	All issues are entered into a production-quality bug tracking system. Items are assigned to developers, for correction, and then tested by QA to ensure proper resolution of issues. a) Patches are not used b) No / NA c) Patches are not used d) NA e) NA

Control Definition	EMS	Pollsite Voting System	Disability Voting System
e) How is the need for patches and updates addressed through the certification/recertification process?			
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.	All known bugs have been addressed as part of the NY certification process.	All known bugs have been addressed as part of the NY certification process.	All known bugs have been addressed as part of the NY certification process.
6) What is the SDLC methodology used in the development of each major component?	An internal SDLC comprising of 15 steps from Ideal to End of Life. Agile techniques are used during the actual product development.	An internal SDLC comprising of 15 steps from Ideal to End of Life. Agile techniques are used during the actual product development.	An internal SDLC comprising of 15 steps from Ideal to End of Life. Agile techniques are used during the actual product development.
7) Describe the process of moving new applications or versions from development to QA, to staging and into production.	Weekly releases of builds for continuous testing with periodic major integration releases for complete testing and bug resolution	Weekly releases of builds for continuous testing with periodic major integration releases for complete testing and bug resolution	Weekly releases of builds for continuous testing with periodic major integration releases for complete testing and bug resolution
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?	Yes. There are 7 checkpoints: System Requirements Base lined, Project Business Review, Next Level Project Requirements, Engineering Test Release, QA Release, Field Test Release, and Certification Release.	Yes. There are 7 checkpoints: System Requirements Base lined, Project Business Review, Next Level Project Requirements, Engineering Test Release, QA Release, Field Test Release, and Certification Release.	Yes. There are 7 checkpoints: System Requirements Base lined, Project Business Review, Next Level Project Requirements, Engineering Test Release, QA Release, Field Test Release, and Certification Release.
9) What checks and balances are in place to ensure that application code does not vary from "approved" versions?	Please refer to VVSG 2005 for source code and application handling requirements of 'approved' versions.	Please refer to VVSG 2005 for source code and application handling requirements of 'approved' versions.	Please refer to VVSG 2005 for source code and application handling requirements of 'approved' versions.

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 storage mechanism for vote results data inside the EMS is the secured database with hashed (non-viewable) results.	The storage mechanism for voting results is the CF card, all encrypted in a binary structure type.	The storage mechanism for voting results is the CF card, all encrypted in a binary structure type.
2) What integrity checks are built-in to ensure the votes cast are the votes recorded?	NA	User review of ballot analysis, stored scanned ballot image with vote analysis summary, audio review of ballot	User review of ballot analysis, stored scanned ballot image with vote analysis summary, audio review of ballot
3) What mechanism is in place to ensure that there is a clear one-to-one correspondence between ballots cast and all electronic records?	Same as above.	Same as above.	Same as above.
4) Where are the aggregated vote totals stored (please discuss physical and logical mechanisms)	Aggregated vote totals are stored in the database separated by tabulator and added up during report generation.	Proprietary binary storage format stored on primary and secondary compact flash devices	Proprietary binary storage format stored on primary and secondary compact flash devices
5) How is access to the EMS (central vote tally) controlled, i.e. what types of access control prevents access to the underlying data?	OS level login and password, DB login and password, and application (EMS) login and password. All are securely stored, recorded and audible.	NA	NA
6) What controls prevent tampering with vote results at pollsites?	NA	Tamper-proof seals are used on the equipment. Results and images are signed and encrypted incrementally as votes are cast. Changes to results will result in a hash check failure.	Tamper-proof seals are used on the equipment. Results and images are signed and encrypted incrementally as votes are cast. Changes to results will result in a hash check failure.

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>	NA	<p>A) Paper ballots are stored inside locked ballot box</p> <p>B) Multiple possibilities:</p> <p>1) Re-feed ballots</p> <p>2) Examine ballot images</p> <p>3) Hand count of all paper ballots</p>	<p>A) Paper ballots are stored inside locked ballot box</p> <p>B) Multiple possibilities:</p> <p>1) Re-feed ballots</p> <p>2) Examine ballot images</p> <p>3) Hand count of all paper ballots</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>Encrypted CF memory cards are verified and loaded (single step) into the EMS system after the polls close and delivered.</p>	<p>The primary CF card needs to be extracted (following procedure) after the polls are closed and brought to the EMS location. Secondary cards should also be conveyed to EMS location in case the backup is needed</p>	<p>The primary CF card needs to be extracted (following procedure) after the polls are closed and brought to the EMS location. Secondary cards should also be conveyed to EMS location in case the backup is needed</p>
<p>9) What controls are in place to assure that the results (memory card, CD etc.) which leave the pollsite are the same as those entered into the EMS</p>	<p>The EMS system will verify the integrity of the CF card and its data during the uploading procedure by decrypting the results files and also checking the hash for integrity.</p>	NA	NA
<p>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?</p>	NA	<p>All information is single point entry and storage; there are no exports, bridges, or linkages which could introduce error or vulnerability. Accuracy is verified during certification and then again during customer LAT.</p>	<p>All information is single point entry and storage; there are no exports, bridges, or linkages which could introduce error or vulnerability. Accuracy is verified during certification and then again during customer LAT.</p>
<p>11) What types of integrity controls are in place to assure that results have not been tampered with at the pollsite?</p>	NA	<p>Multiple security techniques including encrypted election files and results, tamper-proof seals and locks.</p>	<p>Multiple security techniques including encrypted election files and results, tamper-proof seals and locks.</p>

Control Definition	EMS	Pollsite Voting System	Disability Voting System
12) What types of integrity controls are in place to assure that results have not been tampered with at the EMS location?	The EMS software has built-in integrity checking tools for voting results. Microsoft SQL 2005 also has integrity and auditing tools available.	NA	NA
13) What types of access controls are in place to assure security and integrity of the application and associated modules? d) What Authentication mechanisms are used? e) What is the Authorization Matrix? Detail the access to data. a) Do you use role-based access control? Are access permissions based upon defined roles?	Login and password authentication mechanisms are used. We use role-based access control and each action available in the EMS system (add, remove, edit, execute, etc.) has an individual check box for "allow or don't allow".	The poll site tabulator uses security keys containing discrete encryption keys which allow authenticated users to open, close and perform diagnostics. Access is not user defined.	The poll site tabulator uses security keys containing discrete encryption keys which allow authenticated users to open, close and perform diagnostics. Access is not user defined.
14) What is the end-to-end chain-of-custody for the software and firmware in each component?	VSTL → State Body → County, verification can happen at all points.	VSTL → State Body → County, verification can happen at all points.	VSTL → State Body → County, verification can happen at all points.
15) How do the Pollsite Voting System and the EMS prevent the introduction of results from other jurisdictions' election definitions, ballots, and results?	The EMS system has recorded independent security codes on each tabulator that would restrict use of another, non-valid (for that jurisdiction) voting result.	The EMS system has recorded independent security codes on each tabulator that would restrict use of another, non-valid (for that jurisdiction) voting result.	The EMS system has recorded independent security codes on each tabulator that would restrict use of another, non-valid (for that jurisdiction) voting result.

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 	<ul style="list-style-type: none"> a) The vendor does not provide code directly to Counties, so in order for this to be successful the hacker would have to submit the malicious code to the State Board and use them to authorize and distribute the code. b) A change to the aggregated results will result in the EMS system detecting an error and immediately identifying a breach. 	<ul style="list-style-type: none"> a) The vendor does not provide code directly to Counties, so in order for this to be successful the hacker would have to submit the malicious code to the State Board and use them to authorize and distribute the code. b) A change to the poll results will be immediately visible evident to all observers, plus the system will detect an error and cease operation. 	<ul style="list-style-type: none"> a) The vendor does not provide code directly to Counties, so in order for this to be successful the hacker would have to submit the malicious code to the State Board and use them to authorize and distribute the code. b) A change to the poll results will be immediately visible evident to all observers, plus the system will detect an error and cease operation.
<p>2) What is the process for analyzing identified risks and developing countermeasures or mitigating controls to identified risks and vulnerabilities?</p>	<p>Dominion maintains risk registers of all risks and vulnerabilities. We perform Open Ended Vulnerability Testing for all known vulnerabilities, requirements, and internally devised threat possibilities.</p>	<p>Dominion maintains risk registers of all risks and vulnerabilities. We perform Open Ended Vulnerability Testing for all known vulnerabilities, requirements, and internally devised threat possibilities.</p>	<p>Dominion maintains risk registers of all risks and vulnerabilities. We perform Open Ended Vulnerability Testing for all known vulnerabilities, requirements, and internally devised threat possibilities.</p>
<p>3) What tools do the systems provide to support re-canvassing and statistically validating election results?</p>	<p>EMS overall has complete audit module functionality built in to each instance including custom report generation, full field search capability, and XML/EML exporting to any source of statistical election validation (various confidence formulas).</p>	<p>EMS has complete audit module functionality per poll site built in to each instance including custom report generation, full field search capability, and XML/EML exporting to any source of statistical election validation (various confidence formulas).</p>	<p>EMS has complete audit module functionality per poll site built in to each instance including custom report generation, full field search capability, and XML/EML exporting to any source of statistical election validation (various confidence formulas).</p>