

BOE in NYC
RFI for Voting System
Addendum # 2
Additional Security Questions
for
Insert Vendor Name & Product

January 3, 2009

Table of Contents

Physical Security	2
Operating System Security	3
Data Security.....	4
Network Security	7
Application Development Security.....	8
Application Functional Security	9
Miscellaneous	12

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
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) <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 			
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?			
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?			
4) Please list all ports on the unit with descriptions of form factors, communication protocols and purpose			

Control Definition	EMS	Pollsite Voting System	Disability Voting System
5) What capability is in place to secure ports from access by unauthorized connections, e.g. connecting a portable computing unit to the ports			
6) Are all modular and removable components (such as printers and memory modules) serialized to track system assemblies and sub assemblies?			

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.			
2) Is there a standardized process for hardening of operating system components prior to delivery to the board of elections? <ul style="list-style-type: none"> 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? 			
3) What is the mechanism and process used to install the operating system?			
4) How are announced security vulnerabilities addressed?			

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<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? 			
<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 modules d) Turning services on or off 			

Data Security

Control Definition	EMS	Pollsite Voting System	Disability Voting System
--------------------	-----	------------------------	--------------------------

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.			
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?			
3) Are data-specific security counter-measures implemented, e.g. database firewalls, database auditing tools?			
4) In cases where data may be used for development, is data abstracted before being moved into development?			
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?			
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?			

Control Definition	EMS	Pollsite Voting System	Disability Voting System
<p>7) How are announced security vulnerabilities addressed?</p> <ul style="list-style-type: none"> 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? 			
<p>8) What applications are used to create reports directly from the data? How is security of the reporting applications maintained?</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
1) Do any of the major components have physical network connections available? Could physical network connections be installed without detection?			
2) If any of the above received a “YES”, please describe in detail countermeasures used to ensure that only authorized connectivity can occur.			
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?			
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.			
5) What kinds of network security does the system provide to support networking capabilities that may be added later?			

Application Development Security

Control Definition	EMS	Pollsite Voting System	Disability Voting System
1) What development platform(s) were utilized for each major component?			
2) Is source code available for public review?			
3) What is your internal process for testing applications? Are the results of internal testing publicly available?			
<ul style="list-style-type: none"> 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? 			
<ul style="list-style-type: none"> 4) What is the process for patching bugs or security vulnerabilities in the applications? <ul style="list-style-type: none"> 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 e) How is the need for patches and updates addressed through the certification/recertification process? 			

Control Definition	EMS	Pollsite Voting System	Disability Voting System
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.			
6) What is the SDLC methodology used in the development of each major component?			
7) Describe the process of moving new applications or versions from development to QA, to staging and into production.			
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?			
9) What checks and balances are in place to ensure that application code does not vary from “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?			
2) What integrity checks are built-in to ensure the votes cast are the votes recorded?			
3) What mechanism is in place to ensure that there is a clear one-to-one correspondence between ballots cast and all electronic			

Control Definition	EMS	Pollsite Voting System	Disability Voting System
records?			
4) Where are the aggregated vote totals stored (please discuss physical and logical mechanisms)			
5) How is access to the EMS (central vote tally) controlled, i.e. what types of access control prevents access to the underlying data?			
6) What controls prevent tampering with vote results at pollsites?			
7) Describe the canvass process a) Where are the physical paper ballots stored after they are cast at the pollsite? b) What is the proscribed method for conducting an audit?			
8) What is the mechanism and process for moving vote tallies and associated data from the pollsite voting systems to the EMS system?			
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			
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?			

Control Definition	EMS	Pollsite Voting System	Disability Voting System
11) What types of integrity controls are in place to assure that results have not been tampered with at the pollsite?			
12) What types of integrity controls are in place to assure that results have not been tampered with at the EMS location?			
13) What types of access controls are in place to assure security and integrity of the application and associated modules? a) What Authentication mechanisms are used? b) 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?			
14) What is the end-to-end chain-of-custody for the software and firmware in each component?			
15) How do the Pollsite Voting System and the EMS prevent the introduction of results from other jurisdictions' election definitions, ballots, and results?			

Miscellaneous

Control Definition	EMS	Pollsite Voting System	Disability Voting System
1) What is the process for addressing potential breaches of system security, i.e. incident response – possible scenarios would be: <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 			
2) What is the process for analyzing identified risks and developing countermeasures or mitigating controls to identified risks and vulnerabilities?			
3) What tools do the systems provide to support re-canvassing and statistically validating election results?			