Appendix C – VSTLs' Comments to the UPPTR

VSTL Comments to UPPTR Section 2 (Functional Requirements)

SLI's Comments to the UPPTR Section 2 (Functional Requirements)

Section	Requirements	SLI Comments
2.1 Accuracy		
2.1 Accuracy	The voting system SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	"Shall" should be removed from header
2.1.1 Components and Hardware		
2.1.1.1 Component accuracy	Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate.	1) Standards are recommended to specify appropriate component accuracy 2) This is better suited to Inspection, viewing the results overall of the testing, as well as review of hardware manufacturer specifications
2.1.1.2 Equipment design	The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy.	This should be Inspection / Review of hardware test reports and/or hardware specifications.
2.1.1.3 Voting system accuracy	To ensure vote accuracy, all voting systems SHALL:	
2.1.1.3 Voting system accuracy	a. Record the election contests, candidates, and issues exactly as defined by election officials;	
2.1.1.3 Voting system accuracy	b. Record the appropriate options for casting and recording votes;	
2.1.1.3 Voting system accuracy	c. Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast;	
2.1.1.3 Voting system accuracy	d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy;	1) Recommend this as Inspection. 2) Best suited for a source code review and environment specification, in particular for data at rest.
2.1.1.3 Voting system accuracy	e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.	1) Recommend this as Inspection. As written, this requirement is only looking to verfiy that the monitoring software is provided. 2) Would recommend that the "...and how they were corrected." portion be broken out to another requirement, as this looks to be more of an event log.
2.1.2 Environmental Range	All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions.	This should be Inspection / Review of hardware test reports and/or hardware specifications. As written this requirement seems to be written more for a traditional voting system than a UOCAVA internet based system.
2.1.3 Content of Data Verified for Accuracy		

VSTL Comments to UPPTR Section 5 (Security)

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.1 Access Control	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.	Manufacturer shall clearly define what level users, roles and groups are defined on, whether that be at the operating system or the voting system level	
5.1.1 Separation of Duties			
5.1.1.1 Definition of roles	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	Agree with Requirement	Specific roles should be defined to facilitate true segregation of duties.
5.1.1.2 Access to election data	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	Agree with Requirement	No recommended change
5.1.1.3 Separation of duties	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	Enumerate the activities	Current web based system do not do tabulation so this requirement was not applicable to our testing. The majority of election configuration is done independent of the Web application and is therefore not a critical function of our testing.
5.1.2 Voting System Access	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated	This requirement does not define at what minimum level this security should be implemented.
5.1.2.1 Identity verification	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	This requirement should be split out. It covers both authentication and authorization.	This requirement does not define at what minimum level this security should be implemented.
5.1.2.2 Access control configuration	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Enumerate the activities	This requirement does not state whether this should be a system OS level or at a web based administration application level.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.1 Access Control	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.	Manufacturer shall clearly define what level users, roles and groups are defined on, whether that be at the operating system or the voting system level	
5.1.1 Separation of Duties			
5.1.1.1 Definition of roles	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	Agree with Requirement	Specific roles should be defined to facilitate true segregation of duties.
5.1.1.2 Access to election data	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	Agree with Requirement	No recommended change
5.1.1.3 Separation of duties	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	Enumerate the activities	Current web based system do not do tabulation so this requirement was not applicable to our testing. The majority of election configuration is done independent of the Web application and is therefore not a critical function of our testing.
5.1.2 Voting System Access	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated	This requirement does not define at what minimum level this security should be implemented.
5.1.2.1 Identity verification	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	This requirement should be split out. It covers both authentication and authorization.	This requirement does not define at what minimum level this security should be implemented.
5.1.2.2 Access control configuration	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Enumerate the activities	This requirement does not state whether this should be a system OS level or at a web based administration application level.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.1.2.3 Default access control configuration	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	Agree with Requirement	No recommended change
5.1.2.4 Escalation prevention	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	Agree with Requirement	No recommended change
5.1.2.5 Operating system privileged account restriction	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	Should enumerate the activities	Wyle's testing was based on utilization of a web based application. Therefore this did not apply directly. But, it was noted that in some systems tested the OS administration privileges were required to configure election information.
5.1.2.6 Logging of account	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	This is tested in 5.6.3.3	This requirement does not define what information should be logged. Some systems only log Administration functions while others only log Voter information.
5.1.2.7 Monitoring voting system access	The((voting system))SHALL provide tools ((or shall be provided)) for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	Should enumerate the activities. Concern for this requirement is if it is realistically feasible to monitor a globally distributed system, with potentially a very large set of users	This requirement does not define what information should be logged. This requirement also does not state if the tool is to be accessible via the Web based administration application or at an OS Level.
5.1.2.8 Login failures	The vote capture devices at the kiosk locations and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures.	1) SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated. 2) Enumerate activities 3) This requirement is too specific, should use the term "voting system" so that all areas are covered	This requirement does not define if this needs to be at a Web application level or at OS level. Reactivation of an account should not require utilization of anything but the Web based application.
5.1.2.8 Login failures	a. The lockout threshold SHALL be configurable by appropriate administrators/operators.	Agree with Requirement	not broken out
5.1.2.8 Login failures	b. The voting system SHALL log the event.	Covered in 5.6.3.3	not broken out
5.1.2.8 Login failures	c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event.	Agree with Requirement	not broken out

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.1.2.8 Login failures	d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	Agree with Requirement	not broken out
5.1.2.9 Account lockout logging	The voting system SHALL log a notification when any account has been locked out.	Covered in 5.6.3.3	This requirement does not define what information should be logged.
5.1.2.10 Session time-out	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	Enumerate activities	This requirement does not define how this function should be configured.
5.1.2.11 Screen lock	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked	Should mention need for re-authentication in order to re-access	This requirement was deemed N/A due to the web based application being accessible from a privately controlled PC and not a public Voting site.
5.2 Identification and Authentication			
5.2.1 Authentication			
5.2.1.1 Strength of authentication	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	This should be referring to appropriate NIST SP, NIST 800-63 Electronic Authentication Guideline Standards.	
5.2.1.2 Minimum authentication methods	The voting system SHALL authenticate users per the minimum authentication methods outlined below.		Since these systems do not tabulate and are not located in a polling location, the groups for Election Judge and Kiosk Worker do not really apply. (See Table 5-1 Roles : Section 5 | Page 59.)
5.2.1.2 Minimum authentication methods	Election Judge Two factor	Agree with Requirement	
5.2.1.2 Minimum authentication methods	Kiosk Worker One factor	Agree with Requirement	
5.2.1.2 Minimum authentication methods	Voter Not required	Assuming voter authentication is performed "outside" the scope of the voting system, by kiosk worker/Election Official	
5.2.1.2 Minimum authentication methods	Election Official Two factor	Agree with Requirement	
5.2.1.2 Minimum authentication methods	Administrator Two factor	Agree with Requirement	
5.2.1.2 Minimum authentication methods	Application or Process Digital signature 112 bits of security1	Agree with Requirement	
5.2.1.3 Multiple authentication mechanisms	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	Agree with Requirement	This requirement does not define what minimum level is required.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.2.1.4 Secure storage of authentication data	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	Agree with Requirement	
5.2.1.5 Password reset	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	Covers passwords only. What if there are alternative methods of authentication?	This requirement does not define if this function is to be Web Based.
5.2.1.6 Password strength configuration	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	Should specify the authentication level as defined in reference NIST SP	This requirement does not define if this configuration is to be Web Based or OS configurable.
5.2.1.7 Password history configuration	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system. NIST Special Publication 800-57	Agree with Requirement	This requirement does not define if this configuration is to be Web Based or OS configurable.
5.2.1.8 Account information password restriction	The voting system SHALL ensure that the user name is not used in the password. Cannot be fully verified in lab; Testing at remote voting location(s) at operational level.	Agree with Requirement	
5.2.1.9 Automated password expiration	The voting system SHALL provide a means to automatically expire passwords.	Agree with Requirement	
5.2.1.10 Device authentication	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	Tested in 5.3.1.2	This requirement does not define which NIST standard or level to use.
5.2.1.11 Network authentication	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security. Cannot be fully verified in lab; Testing at remote voting location(s) at operational level	Tested in 5.3.1.2	Wyle deems this requirement N/A due to the Web Based architecture. VPN systems will only be utilized at a system server level.
5.2.1.12 Message authentication	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	1) need to define what is a "message" 2) Tested in 5.3.1.2	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.2.1.13 Message authentication mechanisms	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	1) Is the intent here to use current certified communication methodologies? If so, would be better suited as an Inspection test method 2) Tested in 5.3.1.1 and 5.3.1.3 and 5.3.2.4	
5.3 Cryptography		1) SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated. 2) Note quantify "Strong Authentication", this term is too vague, should reference a standard	
5.3.1 General Cryptography Requirements		This section needs additional requirements that handle the situation of keys purchase from a Certificate Authority	
5.3.1.1 Cryptographic functionality	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols	"… or use published and credible cryptographic algorithms/schemas/protocols " is something that should be qualified by FVAP/NIST. Preference is to not leave it to a VSTL to determine, or leave as a loophole for a manufacturer to argue.	This requirement does not define what minimum NIST level is required.
5.3.1.2 Required security strength	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	Agree with Requirement	
5.3.1.3 Use NIST-approved cryptography for communications	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	These requirements should be split out to discrete items	This requirement does not define which NIST standard or level to use.
5.3.2 Key Management	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1 Key generation methods	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	See comment on 5.3.1.1, as it is applicable here as well	This requirement does not define which NIST standard or level to use.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.3.2.2 Security of key generation methods	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	Agree with Requirement	
5.3.2.3 Seed values	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	These requirements should be split out to discrete items	
5.3.2.4 Use NIST-approved key generation methods for communications	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	1) These requirements should be split out to discrete items 2) Unless key is purchased from a Certificate Authority	This requirement does not define which NIST standard or level to use.
5.3.2.5 Random number generator health tests	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	Agree with Requirement	
5.3.3 Key Establishment	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.	Agree with Requirement	
5.3.3.1 Key entry and output	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	Agree with Requirement	
5.3.4 Key handling			
5.3.4.1 Key storage	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	These requirements should be split out to discrete items	
5.3.4.2 Key zeroization	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	Agree with Requirement	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.3.4.3 Support for rekeying	`	What is the acceptable level of effort to reset the cryptographic keys to new values? Is it acceptable to have to redefine the election? Or should the jurisdiction be able to just replace the keys?	
5.4 Voting System Integrity Management		This section has difficulty when applied to "ballot delivery" systems. Would work better to have 5.4.1 be specific to vote capture devices, then have a section 5.4.2 that pertains to vote capture devices and ballot delivery systems	
5.4.1 Protecting the Integrity of the Voting System		May need an additional requirement for nonrepudiation issues	
5.4.1.1 Cast vote integrity; transmission	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	Agree with Requirement	
5.4.1.2 Cast vote integrity; storage	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	Agree with Requirement	
5.4.1.3 Cast vote storage	Cast vote data SHALL NOT be permanently stored on the vote capture device	For the kiosk environment this works fine. If this is ever applied beyond section 1.1.3, to personal computers being used as the vote capture device, then there will be issues with regards to how the configuration is regulated.	
5.4.1.4 Electronic ballot box integrity	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Additional detailed definition of "electronic ballot box" is needed.	
5.4.1.5 Malware detection	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications	More definition is needed to quantify the level of protection needed. Potentially a hardware/software malware detection solution, instead of just software.	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.4.1.6 Updating malware detection	The voting system SHALL provide a mechanism for updating malware detection signatures.	A follow on requirement to this one would be to have the manufacturer specify in their documentation (i.e. an Inspection test method) the recommend interval for requiring updated signatures	
5.4.1.7 Validating software on kiosk voting devices	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	This requirement needs to be expanded to cover all associated devices at the kiosk location. Some systems contain additional devices.	Wyle deems this requirement N/A due to the Web Based architecture.
5.5 Communications Security	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.	Some of the requirements in this section appear to explicitly call out specific communication protocols, which could be interpreted to exclude all other like communication protocols.	
5.5.1 Data Transmission Integrity			
5.5.1.1 Data integrity protection	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	Recommend that this requirement be broken out to handle outbound versus inbound separately	
5.5.1.2 TLS/SSL	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0). verify all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	Agree with Requirement	
5.5.1.3 Virtual private networks (VPN)	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	Tested in 5.3.1.1 and 5.3.1.3. As this appears to be a specific instance of the above mentioned requirements, would recommend removal in order to reduce redundancy.	Wyle deems this requirement N/A due to the Web Based architecture. VPN systems will only be utilized at a system server level.
5.5.1.4 Unique system identifier	Each communicating device SHALL have a unique system identifier	Agree with Requirement	
5.5.1.5 Mutual authentication required	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	Recommend referencing appropriate NIST publication (SP 800-63) to more clearly define "mutually strongly authenticate"	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.5.1.6 Secrecy of ballot data	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	1) This requirement should be split out 2) Recommend more clearly state that voter data is to be encrypted. "Preserve the secrecy …" creates ambiguity.	
5.5.2 External Threats	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	"SHALL" should be removed from header	
5.5.2.1 Disabling network interfaces	Voting system components SHALL have the ability to enable or disable physical network interfaces.	Agree with Requirement	
5.5.2.2 Minimizing interfaces	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	Need to define test method "Inspection/Vulnerability"	
5.5.2.3 Prevention of attacks and security non-compliance	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	Make this 5.5.2.4 need to define test method "Functional/Vulnerability"	
5.6 Logging			
5.6.1 Log Management			
5.6.1.1 Default settings	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1) This should be split to more discrete sub requirements 2) term "default settings" is ambiguous, should require "minimal settings" as per NIST SP 800-92	
5.6.1.2 Log access	Logs SHALL only be accessible to authorized roles	Term "authorized roles" is undefined within the requirements. This should be more clearly defined	
5.6.1.3 Log access	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	Term "privileged logging processes" is undefined within the requirements. This should be more clearly defined	
5.6.1.4 Logging events	The voting system SHALL log logging failures, log clearing, and log rotation.	This should be split out to discrete 3 sub-requirements	This requirement does not specify if these logs should contain both voter and administration information.
5.6.1.5 Log format	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	Agree with Requirement	This requirement does not determine if these functions should be part of an administration web based application or at an OS level administration function.
5.6.1.6 Log separation	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	This should be split out to discrete 2 sub-requirements	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.1.7 Log review	The voting system SHALL include an application or program to view, analyze, and search event logs.	This should be split out to 3 discrete sub-requirements	This requirement does not determine if these functions should be part of an administration web based application or at an OS level administration function.
5.6.1.8 Log preservation	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	Term "prior to voting system decommissioning" is ambiguous. We believe the intent is that the log data remains intact for the life cycle of the given election data for a particular election. This may be defined at the jurisdictional level.	
5.6.1.9 Voter privacy	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	Agree with Requirement	This requirement does not outline what information is deemed to violate a voter's identity. These systems utilize several voter specific credentials that are required for proper identification of voters.
5.6.1.10 Timekeeping format	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds	Agree with Requirement	
5.6.1.11 Timekeeping precision	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	Agree with Requirement	This requirement must meet 5.6.1.10
5.6.1.12 System clock security	Only the system administrator SHALL be permitted to set the system clock	Would recommend that the "system administrator" role be changed to indicate an appropriately authorized election official	Wyle determined that this requirement is N/A due to this function being a system administration function.
5.6.2 Communications Logging			
5.6.2.1 General	All communications actions SHALL be logged.	Agree with Requirement	This requirement does not define what all communications encompasses.
5.6.2.2 Log content	The communications log SHALL contain at least the following entries:	1) Enumerate, not using bullets, must be able to explicitly reference 2) Similar to 5.6.3.1, test method should be Inspection	
5.6.2.2 Log content	Times when the communications are activated and deactivated;	Agree with Requirement	
5.6.2.2 Log content	Services accessed;	Agree with Requirement	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.2.2 Log content	Identification of the device which data was transmitted to or received from;	Agree with Requirement	
5.6.2.2 Log content	Identification of authorized entity; and	Agree with Requirement	
5.6.2.2 Log content	Successful and unsuccessful attempts to access communications or services.	Agree with Requirement	
5.6.3 System Event Logging	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		
5.6.3.1 Event log format	The voting system SHALL log the following data for each event:	Agree with Requirement	
5.6.3.1 Event log format	a. System ID;	Agree with Requirement	
5.6.3.1 Event log format	b. Unique event ID and/or type;	Agree with Requirement	
5.6.3.1 Event log format	c. Timestamp;	Agree with Requirement	
5.6.3.1 Event log format	d. Success or failure of event, if applicable;	Agree with Requirement	
5.6.3.1 Event log format	e. User ID triggering the event, if applicable; and	Agree with Requirement	
5.6.3.1 Event log format	f. Jurisdiction, if applicable.	Agree with Requirement	
5.6.3.2 Critical events	All critical events SHALL be recorded in the system event log.	Define a critical event. The requirement as it is now leaves room for interpretation in regards to the scope of the requirement	This requirement does not define what a critical event might be.
5.6.3.3 System events	At a minimum the voting system SHALL log the events described in Table 5-2. (The contents of the table appear in this list under the 5.6.3.3 heading)	This section would be better served to be broken out into subparagraphs. Referencing back to a row, or a bullet in a cell is many times problematic Additionally the requirement only states "voting system" this is a broad scope of equipment and software. Does this apply to the O/S, The voting system application, or both? General Comment for this table would be to recommend that the term "include but not limited to" be avoided, as this term creates ambiguity and potential for inconsistent interpretation of the requirement	Wyle was unable to completely validate this requirement due to limited access to physical hardware. The majority of the events defined are from a server OS level and not a web based application level.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.3.3.a1 Error and exception messages	The source and disposition of system interrupts resulting in entry into exception handling routines.	System interrupts at an operating system / hardware level could be potentially destructive. Source code can be analyzed for an understanding of exception handling routines then a script can be written to invoke a system interrupts that would result in an entry into exception handling routines.	
5.6.3.3.a2	Messages generated by exception handlers.	Agree with Requirement	
5.6.3.3.a3	The identification code and number of occurrences for each hardware and software error or failure.	Agree with Requirement	
5.6.3.3.a4	Notification of physical violations of security.	the term "physical violations of security" needs to be better defined as to what is included. I.e. computer room security, motion sensors, chassis alarms, etc.	
5.6.3.3.a5	Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies.	Agree with Requirement	
5.6.3.3.a6	All faults and the recovery actions taken.	the term "fault" is ambiguous, needs to be more clearly defined.	
5.6.3.3.a7	Error and exception messages such as ordinary timer system interrupts and normal I/O system interrupts do not need to be logged.	define "ordinary", and seems to be in conflict with bullet 2	
5.6.3.3.b	Critical system status messages	1) More detail/criteria is needed to define what is considered critical. "includes but not limited to" creates a large potential for gaps to occur, as well as disagreements by a manufacturer as to what is deemed critical.	
5.6.3.3.b1	Critical system status messages other than information messages displayed by the device during the course of normal operations. Includes but not limited to: Diagnostic and status messages upon startup.	Agree with Requirement Though Diagnostics and status messages upon startup do not seem to be critical type message	
5.6.3.3.b2	The “zero totals” check conducted before starting the voting period.	Agree with Requirement	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.3.3.c Non-critical status messages	Non-critical status messages Non-critical status messages that are generated by the data quality monitor or by software and hardware condition monitors.	1) need better criteria for determining what is non-critical versus what is critical status messages. 2) need clarification as to what is meant by "data quality monitor". This term seems to be very subjective and open to interpretation. Likely to cause significant disagreement as to what is	
5.6.3.3.d Events that require election official intervention	Events that require election official intervention Events that require election official intervention, so that each election official access can be monitored and access sequence can be constructed.	Agree with Requirement	
5.6.3.3.e shutdown and restarts	Shutdown and restarts Both normal and abnormal shutdowns and restarts.	Recommend adding "Power up" to this line item	
5.6.3.3.f Changes to system configuration settings	Changes to system configuration settings Configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other system configuration settings.	Recommend additional specificity , rather than alluding to "other system configuration settings"	
5.6.3.3.g Integrity checks for executables, configuration files, data and logs	Integrity checks for executables, configuration files, data, and logs Integrity checks that may indicate possible tampering with files and data.	Should explicitly call out "logs" in description	
5.6.3.3.h The addition and deletion of files	The addition and deletion of files Files added or deleted from the system.	Recommend additional detail as to file types. Would not recommend having to track temporary files that are automatically handled within the system	
5.6.3.3.i1 System readiness results	System readiness results Includes but not limited to: System pass or fail of hardware and software test for system readiness.	Agree with Requirement	
5.6.3.3.i2	Identification of the software release, identification of the election to be processed, kiosk locations, and the results of the software and hardware diagnostic tests.	Agree with Requirement	
5.6.3.3.13	Pass or fail of ballot style compatibility and integrity test.	Agree with Requirement	
5.6.3.3.i4	Pass or fail of system test data removal.	Agree with Requirement	
5.6.3.3.j Removable media events	Removable media events Removable media that is inserted into or removed from the system.	Agree with Requirement	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.3.3.k Backup and restore	Backup and restore Successful and failed attempts to perform backups and restores.	Agree with Requirement	
5.6.3.3.l1 Authentication related events	Authentication related events Includes but not limited to: Login/logoff events (both successful and failed attempts).	Agree with Requirement	
5.6.3.3.l2	Account lockout events.	Agree with Requirement	
5.6.3.3.l3	Password changes.	Agree with Requirement	
5.6.3.3.m1 Access control related events	Access control related events Includes but not limited to: Use of privileges.	Agree with Requirement	
5.6.3.3.m2	Attempts to exceed privileges.	Agree with Requirement	
5.6.3.3.m3	All access attempts to application and underlying system resources.	Recommend removal of "…and underlying system resources", as this is beyond the scope of the voting system applications logging scope.	
5.6.3.3.m4	Changes to the access control configuration of the system.	Agree with Requirement	
5.6.3.3.n1 User account and role (or groups) management activity	User account and role (or groups) management activity Includes but not limited to: Addition and deletion of user accounts and roles.	Agree with Requirement	
5.6.3.3.n2	User account and role suspension and reactivation.	Agree with Requirement	
5.6.3.3.n3	Changes to account or role security attributes such as password length, access levels, login restrictions, permissions.	Agree with Requirement	
5.6.3.3.n4	Administrator account and role password resets.	Agree with Requirement	
5.6.3.3.o Installation, upgrading, patching, or modification of software or firmware	Installation, upgrading, patching, or modification of software or firmware Logging for installation, upgrading, patching, or modification of software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data.	1) This line item needs to be explicitly broken out to individual requirements. The potential scope is very large. In an initial certification, upgrading/patching/modification may well not be available. 2) "Cryptographic hash" needs to be defined. Would recommend using "hash code" instead.	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.3.3.p1 Changes to configuration settings	Changes to configuration settings Includes but not limited to: Changes to critical function settings. At a minimum critical function settings include location of ballot definition file, contents of the ballot definition file, vote reporting, location of logs, and system configuration settings.	This requirement should be split out to more explicitly address either voting system applications or the underlying operating system	
5.6.3.3.p2	Changes to settings including but not limited to enabling and disabling services.	This requirement should be split out to more explicitly address either voting system applications or the underlying operating system.	
5.6.3.3.p3	Starting and stopping processes.	This requirement should be split out to more explicitly address either voting system applications or the underlying operating system	
5.6.3.3.q Abnormal process exits	Abnormal process exits All abnormal process exits.	Agree with Requirement	
5.6.3.3.r Successful and failed database connection attempts (if a database is utilized)	Successful and failed database connection attempts (if a database is utilized). All database connection attempts.	Agree with Requirement	
5.6.3.3.s Changes to cryptographic keys	Changes to cryptographic keys At a minimum critical cryptographic settings include key addition, key removal, and re-keying.	Recommend adding "key zeroization"	
5.6.3.3.t1 Voting events	Voting events Includes: Opening and closing the voting period.	Recommend including successful delivery of appropriate ballot style to voter Agree with Requirement	
5.6.3.3.t2	Casting a vote.	Agree with Requirement	
5.6.3.3.t3	Success or failure of log and election results exportation.	Agree with Requirement	
5.7 Incident Response			
5.7.1 Incident Response Support			

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.7.1.1 Critical events	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	1) Recommend that NIST/FVAP list minimum criteria of what should be classified as critical, in order to create a consistency for this requirement 2) Recommend removal of "e.g." and giving specific criteria that must be met, as in 1) above	Wyle determined that this requirement is not applicable to a web based application. But it is a requirement for a web server and therefore could not be tested at this time.
5.7.1.2 Critical event alarm	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application. A system server notification should be sent to administrators when issues arise with the web server.
5.8 Physical and Environmental Security		Recommend that additional specificity is added to explicitly call out whether each requirement is for the voting system (election creation machines and accumulation/tallying central servers included), or just the vote capture device	
5.8.1 Physical Access			
5.8.1.1 Unauthorized physical access requirement	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.2 Physical Ports and Access Points			
5.8.2.1 Non-essential ports	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	Recommend that "testing" be removed. In a production environment, would not want "test" ports/access points enabled.	
5.8.3 Physical Port Protection			
5.8.3.1 Physical port shutdown requirement	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled	Recommend changing Test Method to Functional	Wyle determined that this requirement is not applicable to a web based application. A physical connection will only be made during a single instance of vote casting.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.8.3.2 Physical component alarm requirement	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	Recommend changing Test Method to Functional	Wyle determined that this requirement is not applicable to a web based application.
5.8.3.3 Physical component event log requirement	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application.
5.8.3.4 Physical port enablement requirement	Disabled ports SHALL only be re-enabled by authorized administrators.	Recommend changing Test Method to Functional	
5.8.3.5 Physical port restriction requirement	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.3.6 Physical port tamper evidence requirement	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.3.7 Physical port disability capability requirement	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.4 Door Cover and Panel Security			
5.8.4.1 Access point security requirement	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	Enumerate the activities	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.5 Secure Paper Record Receptacle			
5.8.5.1 Secure paper record container requirement		Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application
5.8.6 Secure Physical Lock and Key			
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.7 Media Protection	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.	Recommend changing "person privacy related data" to "personally identifiable information (PII)", which is a common industry term	
5.8.7.1 Kiosk site protection	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application.
5.9 Penetration Resistance		Recommend referencing NIST SP dealing with hardening.	
5.9.1 Resistance to Penetration Attempts			
5.9.1.1 Resistant to attempts	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	Recommend defining resistant levels more definitively, and enumerating by device types within a voting system	
5.9.1.2 System information disclosure	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality	1) Recommend defining "appropriate functionality" by device types within a voting system. 2) Recommend referencing NIST SP dealing with hardening.	
5.9.1.3 System access	The voting system SHALL provide no access, information or services to unauthorized entities.	Enumerate the activities	
5.9.1.4 Interfaces	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	Recommend closing all ports and shutting down all services not needed to perform voting activities	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.9.1.5 Documentation	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	Agree with Requirement	Based on the system documentation provided by the participants in this test campaign, Wyle was unable to validate this requirement. However, Wyle deems it necessary for future testing.
5.9.2 Penetration Resistance Test and Evaluation		This section is oriented to the VSTL. As such it should not be in the requirements document that manufacturer's are held to, but in a "Program Manual" that outlines the scope of a certification campaign.	
5.9.2.1 Scope	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following:	Define Test Method "Penetration" versus "Functional"	
5.9.2.1 Scope	System server;	Agree with Requirement	
5.9.2.1 Scope	Vote capture devices;	Agree with Requirement	
5.9.2.1 Scope	Tabulation device;	Agree with Requirement	
5.9.2.1 Scope	All items setup and configured per Technical Data Package (TDP) recommendations;	Agree with Requirement	
5.9.2.1 Scope	Local wired and wireless networks; and	Agree with Requirement	
5.9.2.1 Scope	Internet connections.	Agree with Requirement	
5.9.2.2 Test environment	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	1) This requirement appears to be oriented to the VSTL, not the manufacturer. 2) This may not be feasible for all systems. Have encountered systems that are cloud base, for example.	Wyle was unable to validate this requirement, but deems it necessary for future testing.
5.9.2.3 White box testing	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	1) This requirement appears to be oriented to the VSTL, not the manufacturer. 2) The original text is not a definition of white box testing. 3) With added text, the source code review that would be required would be prohibitive from a cost/benefit viewpoint.	Wyle was unable to validate this requirement, but deems it necessary for future testing.
5.9.2.4 Focus and priorities	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:	1) This requirement appears to be oriented to the VSTL, not the manufacturer.	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	*Requirement*	*SLI Comments*	*Wyle Comments*
5.9.2.4 Focus and priorities	a. Threat scenarios for the voting system under investigation;		
5.9.2.4 Focus and priorities	b. Remote attacks SHALL be prioritized over in-person attacks;		
5.9.2.4 Focus and priorities	c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and		
5.9.2.4 Focus and priorities	d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.		

SLI's Comments to the UPPTR Section 2 (Functional Requirements)

Section	*Requirements*	*SLI Comments*
2.1 Accuracy		
2.1 Accuracy	The voting system SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	"Shall" should be removed from header
2.1.1 Components and Hardware		
2.1.1.1 Component accuracy	Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate.	1) Standards are recommended to specify appropriate component accuracy 2) This is better suited to Inspection, viewing the results overall of the testing, as well as review of hardware manufacturer specifications
2.1.1.2 Equipment design	The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy.	This should be Inspection / Review of hardware test reports and/or hardware specifications.
2.1.1.3 Voting system accuracy	To ensure vote accuracy, all voting systems SHALL:	
2.1.1.3 Voting system accuracy	a. Record the election contests, candidates, and issues exactly as defined by election officials;	
2.1.1.3 Voting system accuracy	b. Record the appropriate options for casting and recording votes;	
2.1.1.3 Voting system accuracy	c. Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast;	
2.1.1.3 Voting system accuracy	d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy;	1) Recommend this as Inspection. 2) Best suited for a source code review and environment specification, in particular for data at rest.
2.1.1.3 Voting system accuracy	e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.	1) Recommend this as Inspection. As written, this requirement is only looking to verfiy that the monitoring software is provided. 2) Would recommend that the "…and how they were corrected." portion be broken out to another requirement, as this looks to be more of an event log.
2.1.2 Environmental Range	All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions.	This should be Inspection / Review of hardware test reports and/or hardware specifications. As written this requirement seems to be written more for a traditional voting system than a UOCAVA internet based system.
2.1.3 Content of Data Verified for Accuracy		

SLI's Comments to the UPPTR Section 2 (Functional Requirements)

Section	*Requirements*	*SLI Comments*
2.1.3.1 Election management system accuracy	Voting systems SHALL accurately record all election management data entered by the user, including election officials or their designees.	As written, this requirement contains a high degree of vagueness. Each type of Election Management data should be enumerated.
2.1.3.2 Recording accuracy	For recording accuracy, all voting systems SHALL:	
2.1.3.2 Recording accuracy	a. Record every entry made by the user except where it violates voter privacy;	
2.1.3.2 Recording accuracy	b. Accurately interpret voter selection(s) and record them correctly to memory;	Recommend that the "… to memory" portion be removed. Is potentially too specific of a data recording method.
2.1.3.2 Recording accuracy	c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory;	It is not clear how this requirement is examining anything different from part b.
2.1.3.2 Recording accuracy	d. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory; and	Our assumption here is that this requirement is testing write-ins as opposed to selecting choices, as in b and c. This requirement (b,c, and d) need to be clarified as to their specific intents, with any redundancies removed.
2.1.3.2 Recording accuracy	e. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals.	2.1.3.2.e would be coverd under EMC testing. This should be Inspection / Review of hardware test reports and/or hardware specifications.
2.1.4 Telecommunications Accuracy	The telecommunications components of all voting systems SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	For telecommunications, if TCP/IP protocols are used all transmissions are guaranteed to be accurate. The discussion of one in ten million and one in half a milion is somewhat obfuscated, the requirement should be more clearly defined stated.

Section	*Requirements*	*SLI Comments*
2.1.5 Accuracy Test Content	Voting system accuracy SHALL be verified by a specific test conducted for this objective. The overall test approach is described in Appendix C.	For a true internet voting system, that uses a web browser implementation for capturing votes, the accuracy test is whether or not the election is coded correctly. The technologies involved are mature, proven and robust. For a true internet voting system that employs physical devices such as a touch screen, the accuracy test would be similar to that of a ballot delivery system, in that the touch screen is dependent on the prescribed maintenance cycle of the device. For a ballot delivery system, where the cast ballot is potentially returned in any of a number or ways (fax, email, printed/scanned), the accuracy is dependent on the device used, within the confines of the prescribed maintenance cycles of the device.
2.1.5.1 Simulators	If a simulator is used, it SHALL be verified independently of the voting system in order to produce ballots as specified for the accuracy testing.	Not a voting system requirement
2.1.5.2 Ballots	Ballots used for accuracy testing SHALL include all the supported types (i.e., rotation, alternative languages) of contests and election types (primary, general).	Question as to the applicability of the ballot type to accuracy testing. Accuracy testing concerns itself with accuracy with regard to the scanning/reading of each possible ballot position on a given size ballot. The ability of the system to correctly handle the various supported voting variations is addressed in other specific tests.
2.1.6 Reporting Accuracy	Processing accuracy is defined as the ability of the voting system to process stored voting data. Processing includes all operations to consolidate voting data after the voting period has ended. The voting systems SHALL produce reports that are consistent, with no discrepancy among reports of voting data.	In general this is a bit high level, would like to see some specific metrics called out to ensure reporting accuracy. Similar v1.0 VVSG volume 1, sections 2.4.2. and 2.4.3
2.2 Operating capacities		

Section	Requirements	SLI Comments
2.2.1 Maximum Capacities	The manufacturer SHALL specify at least the following maximum operating capacities for the voting system (i.e. server, vote capture device, tabulation device, and communications links): - Throughput, - Memory, - Transaction processing speed, and - Election constraints: o Number of jurisdictions o Number of ballot styles per jurisdiction o Number of contests per ballot style o Number of candidates per contest o Number of voted ballots	Recommend that this section look at capacities more in terms of minimums that need to be met (as specified by NIST/FVAP), rather than as stated maximum capacities that a manufacturer claims they can accommodate. Many times a manufacturer will list an unrealistically high number for many of these categories. A minimum standard will create a consistent baseline for all manufacturers.
2.2.1.1 Capacity testing	The voting system SHALL achieve the maximum operating capacities stated by the manufacturer in section 2.2.1.	Recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate within a reasonable cost/benefit ratio.
2.2.2 Operating Capacity notification	The voting system SHALL provide notice when any operating capacity is approaching its limit.	Recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate within a reasonable cost/benefit ratio.
2.2.3 Simultaneous Transmissions	The voting system SHALL protect against the loss of votes due to simultaneous transmissions.	Recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate within a reasonable cost/benefit ratio.
2.3 Pre-Voting Capabilities		
2.3.1 Import and Verify Election Definition		
2.3.1.1 Import the election definition	The voting system SHALL:	
2.3.1.1 Import the election definition	a. Keep all data logically separated by, and accessible only to, the appropriate state and local jurisdictions;	Agree with Requirement
2.3.1.1 Import the election definition	b. Provide the capability to import or manually enter ballot content, ballot instructions and election rules, including all required alternative language translations from each jurisdiction;	Enumerate the activities
2.3.1.1 Import the election definition	c. Provide the capability for the each jurisdiction to verify that their election definition was imported accurately and completely;	Agree with Requirement
2.3.1.1 Import the election definition	d. Support image files (e.g., jpg or gif) andor a handwritten signature image on the ballot so that state seals, official signatures and other graphical ballot elements may be properly displayed; and	Agree with Requirement

Section	*Requirements*	*SLI Comments*
2.3.1.1 Import the election definition	e. Support multiple ballot styles per each local jurisdiction.	Agree with Requirement
2.3.1.2 Protect the election definition	The voting system SHALL provide a method to protect the election definition from unauthorized modification.	Agree with Requirement
2.3.2 Readiness Testing		
2.3.2.1 Voting system test mode	The voting system SHALL provide a test mode to verify that the voting system is correctly installed, properly configured, and all functions are operating to support pre-election readiness testing for each jurisdiction.	Agree with Requirement
2.3.2.2 Test data segregation	The voting system SHALL provide the capability to zero-out or otherwise segregate test data from actual voting data.	Agree with Requirement
2.4 Voting Capabilities		
2.4.1 Opening the Voting Period		
2.4.1.1 Accessing the ballot	The voting system SHALL:	
2.4.1.1 Accessing the ballot	a. Present the correct ballot style to each voter;	Agree with Requirement
2.4.1.1 Accessing the ballot	b. Allow the voting session to be canceled; and	Agree with Requirement
2.4.1.1 Accessing the ballot	c. Prevent a voter from casting more than one ballot in the same election.	Agree with Requirement
2.4.2 Casting a Ballot	The voting system SHALL:	There should be a sub-requirement that deals with the system allowing the voter to change their selection within a contest prior to casting their ballot (similar to (g) for undervotes)
2.4.2.1 Record voter selections	a. Record the selection and non-selection of individual vote choices;	Agree with Requirement
2.4.2.1 Record voter selections	b. Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-ins as the number of candidates the voter is allowed to select;	Recommend splitting sub-requirement so that one validates the ability to enter a write in, and the other verifies that the correct number of write-ins is allowed
2.4.2.1 Record voter selections	c. Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources);	Agree with Requirement
2.4.2.1 Record voter selections	d. Allow the voter to change a vote within a contest before advancing to the next contest;	Agree with Requirement

Section	Requirements	SLI Comments
2.4.2.1 Record voter selections	e. Provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance;	Agree with Requirement
2.4.2.1 Record voter selections	f. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes);	Recommend that this requirement is made more specific as to notifying voter of potential undervote prior to casting of ballot (as opposed to when going from one contest (or screen) to another).
2.4.2.1 Record voter selections	g. Provide the voter the opportunity to correct the ballot for an undervote before the ballot is cast;	Agree with Requirement
2.4.2.1 Record voter selections	h. Allow the voter, at the voter's choice, to submit an undervoted ballot without correction.	Agree with Requirement
2.4.2.1 Record voter selections	i. Prevent the voter from making more than the allowable number of selections for any contest (e.g., overvotes); and	Agree with Requirement
2.4.2.1 Record voter selections	j. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power.	This may not be feasible in a remote session environment. Depending on where the power failure occurs, as well as the duration, will dictate if a ballot can be recorded within the voting system without loss or degradation of voting/audit data. The "… allow voters to resume voting..." clause would inherently cause some kind of voter data to be resident on the vote capture device, which would potentially violate other Security requirements (5.4.1.3)
2.4.2.2 Verify voter selections	The voting system SHALL:	
2.4.2.2 Verify voter selections	a. Produce a paper record each time the confirmation screen is displayed;	Would recommend that a paper record is generated only when the ballot is cast and not each time the confirmation screen is accessed.
2.4.2.2 Verify voter selections	b. Generate a paper record identifier. This SHALL be a random identifier that uniquely links the paper record with the cast vote record;	Agree with Requirement
2.4.2.2 Verify voter selections	c. Allow the voter to either cast the ballot or return to the vote selection process to make changes after reviewing the confirmation screen and paper record; and	Recommend removing "… and paper record", see comment to "a" above.

Section	Requirements	SLI Comments
2.4.2.2 Verify voter selections	d. Prompt the voter to confirm his choices before casting the ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm his intention to cast the ballot.	Agree with Requirement
2.4.2.3 Cast ballot	The voting system SHALL:	Recommend renaming requirement to "Post Cast Ballot Process"
2.4.2.3 Cast ballot	a. Store all cast ballots in a random order; logically separated by, and only accessible to, the appropriate state local jurisdictions;	Agree with Requirement
2.4.2.3 Cast ballot	b. Notify the voter after the vote has been stored persistently that the ballot has been cast;	Recommend defining "persistently" to more detail. In a full electronic system, "persistently" would indicate that the central server has received the vote record and stored it. In a ballot delivery system, "persistently" would indicate the printing of a physical ballot, or creation of a pdf.
2.4.2.3 Cast ballot	c. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, and provide clear instruction as to steps the voter should take to cast his ballot should this event occur; and	Recommend enumerating this requirement to c.i and c.ii
2.4.2.3 Cast ballot	d. Prohibit access to voted ballots until such time as state law allows for processing of absentee ballots.	Agree with Requirement
2.4.2.4 Ballot linking to voter identification		
2.4.2.4.1 Absentee model	The cast ballot SHALL be linked to the voter's identity without violating the privacy of the voter.	Agree with Requirement
2.4.2.4.2 Early voting model	The cast ballot SHALL NOT be linked to the voter's identity.	Agree with Requirement
2.4.3 Vote Secrecy		
2.4.3.1 Link to voter	The voting system SHALL be capable of producing a cast vote record that does not contain any information that would link the record to the voter.	In the Glossary, cast vote record needs a better definition, such that it is differentiated from the cast ballot more explicitly. Should indicate that it is the record stored in the voting system, as opposed to the cast ballot that is produced by the vote capture device. In the Absentee model the cast ballot contains links to the voters identity, where the cast vote record should not.
2.4.3.2 Voting session records	The voting system SHALL NOT store any information related to the actions performed by the voter during the voting session.	Audit logs would record when the voter accessed ballot, as well as when they cast the ballot, but no information that would link stored information to individual voter
2.5 Post Voting Capabilities		

Section	*Requirements*	*SLI Comments*
2.5.1 Ballot Box Retrieval and Tabulation		An additional requirement is recommended that explicitly deals with encryption of electronic ballot box upon closure of the voting period, in order to prevent voter data (private information and vote data) from being exposed in even a read only manner. "Seal" in 2.5.1.1 may be used to cover this concept. But then should be broken out to a seperate requirement from the "sign"
2.5.1.1 Seal and sign the electronic ballot box	The voting system SHALL seal and sign each jurisdiction's electronic ballot box, by means of a digital signature, to protect the integrity of its contents.	Would recommend that the term "seal" be more explicitly defined. "Seal" is historically more of a physical concept, whereas in this instance it is a logical concept. May want to define as making the electronic ballot box "read only", with corresponding time stamp or something similar.
2.5.1.2 Electronic ballot box retrieval	The voting system SHALL allow each jurisdiction to retrieve its electronic ballot box.	Agree with Requirement
2.5.1.3 Electronic ballot box integrity check	The voting system SHALL perform an integrity check on the electronic ballot box verifying that it has not been tampered with or modified before opening.	See comments in 2.5.1 and 2.5.1.1, as would pertain to this requirement
2.5.2 Tabulation		
2.5.2.1 Tabulation device connectivity	The tabulation device SHALL be physically, electrically, and electromagnetically isolated from any other computer network.	Enumerate the activities
2.5.2.2 Open ballot box	The tabulation device SHALL allow only an authorized entity to open the ballot box.	Recommend adding "voting system" in front of "authorized entity"
2.5.2.3 Absentee model		
2.5.2.3.1 Adjudication	The tabulation device SHALL allow the designation of electronic ballots as "accepted" or "not accepted" by an authorized entity.	1) See comment in 2.5.2.2 2) "electronic ballots" is not a defined term. Recommend using the term "Cast Ballot"
2.5.2.4 Ballot decryption	The tabulation device decryption process SHALL remove all layers of encryption and breaking all correlation between the voter and the ballot, producing a record that is in clear text.	Decryption process may be different that what is used to break all correlations between voter and ballot. This requirement should be broken out. The breaking of the correlation should only be done after the adjudication is completed. The decryption process may be involved at multiple points of this overall process.
2.5.2.5 Tabulation report format	The tabulation device SHALL have the capability to generate a tabulation report of voting results in an open and non-proprietary format.	Agree with Requirement

Section	*Requirements*	*SLI Comments*
2.6 Audit and Accountability		Assumption is that 2.6.1 and 2.6.2 are "header" sections that should not have any actionable events. The "Shall" in 2.6.2 should be removed.
2.6.1 Scope	The intention is to provide for independent verification of the agreement of the paper record and electronic tabulation results. These audits could be conducted on the entire set of records or on a sampling basis, depending on the preferences of state/local jurisdictions:	
2.6.1 Scope	a. Hand audit – Validation of electronic tabulation results via comparison with results of a hand tally of paper records; and	
2.6.1 Scope	b. Comparison of ballot images and the corresponding paper records.	
2.6.2 Electronic Records	In order to support independent auditing, a voting system SHALL be able to produce electronic records that contain the necessary information in a secure and usable manner. Typically, this includes records such as: - Vote counts; - Counts of ballots recorded; - Paper record identifier; - Event logs and other records of important events; and - Election archive information.	1) Recommend using appropriate NIST standard, and/or VVSG section 2.1.5, in place of "secure and usable manner". 2) Recommend removing "Typically", and rephrasing to something like, "this includes, but is not limited to:" 3) Enumerate bullets such that they are referenceable. 4) Remove "Shall" as it causes need for actionable event.Recommend more explicity defining "important events"
2.6.2 Electronic Records	The following requirements apply to records produced by the voting system for any exchange of information between devices, support of auditing procedures, or reporting of final results:	Enumerate in relation to above subsection
2.6.2 Electronic Records	a. Requirements for electronic records to be produced by tabulation devices; and	The pertinent requirements associated to this sub requirement should be explicitly called out. A vague reference will only create gaps in coverage.
2.6.2 Electronic Records	b. Requirements for printed reports to support auditing steps.	The pertinent requirements associated to this sub requirement should be explicitly called out. A vague reference will only create gaps in coverage.
2.6.2.1 All records capable of being exported	The voting system SHALL provide the capability to export its electronic records in an open format, such as XML, or include a utility to export log data into a publicly documented format.	Agree with Requirement

Section	*Requirements*	*SLI Comments*
2.6.2.2 Ballot images	The voting system SHALL have the capability to generate ballot images in a human readable format.	Agree with Requirement
2.6.2.3 Ballot image content	The voting system SHALL be capable of producing a ballot image that includes:	Does this requirement need a complementary requirement, similar to how 2.6.3.2 has 2.6.3.3 Privacy?
2.6.2.3 Ballot image content	a. Election title and date of election;	
2.6.2.3 Ballot image content	b. Jurisdiction identifier;	
2.6.2.3 Ballot image content	c. Ballot style;	
2.6.2.3 Ballot image content	d. Paper record identifier; and	
2.6.2.3 Ballot image content	e. For each contest and ballot question:	
2.6.2.3 Ballot image content	i. The choice recorded, including write-ins; and	
2.6.2.3 Ballot image content	ii. Information about each write-in.	
2.6.2.4 All records capable of being printed	The tabulation device SHALL provide the ability to produce printed forms of its electronic records. The printed forms SHALL retain all required information as specified for each record type other than digital signatures.	Should be enumerated or split out
2.6.2.5 Summary count record	The voting system SHALL produce a summary count record including the following:	Agree with Requirement
2.6.2.5 Summary count record	a. Time and date of summary record; and	
2.6.2.5 Summary count record	b. The following, both in total and broken down by ballot style and voting location:	
2.6.2.5 Summary count record	i. Number of received ballots	
2.6.2.5 Summary count record	ii. Number of counted ballots	
2.6.2.5 Summary count record	iii. Number of rejected electronic CVRs	
2.6.2.5 Summary count record	iv. Number of write-in votes	
2.6.2.5 Summary count record	v. Number of undervotes.	
2.6.3 Paper Records	The vote capture device is required to produce a paper record for each ballot cast. This record SHALL be available to the voter to review and verify, and SHALL be retained for later auditing or recounts, as specified by state law. Paper records provide an independent record of the voter's choices that can be used to verify the correctness of the electronic record created by the vote capture device.	Need to remove "Shall" from header
2.6.3.1 Paper record creation	Each vote capture device SHALL print a human readable paper record.	Agree with Requirement
2.6.3.2 Paper record contents	Each paper record SHALL contain at least:	2.6.2.3 and 2.6.3.2 test for the same thing, but one if Test Method Inspection and the other is Functional. Should be consistent. Recommend making both Inspection.

Section	Requirements	SLI Comments
2.6.3.2 Paper record contents	a. Election title and date of election;	
2.6.3.2 Paper record contents	b. Voting location;	
2.6.3.2 Paper record contents	c. Jurisdiction identifier;	
2.6.3.2 Paper record contents	d. Ballot style;	
2.6.3.2 Paper record contents	e. Paper record identifier; and	
2.6.3.2 Paper record contents	f. For each contest and ballot question:	
2.6.3.2 Paper record contents	i. The recorded choice, including write-ins; and	
2.6.3.2 Paper record contents	ii. Information about each write-in.	
2.6.3.3 Privacy	The vote capture device SHALL be capable of producing a paper record that does not contain any information that could link the record to the voter.	Agree with Requirement
2.6.3.4 Multiple pages	When a single paper record spans multiple pages, each page SHALL include the voting location, ballot style, date of election, and page number and total number of the pages (e.g., page 1 of 4).	Enumerate the activities
2.6.3.5 Machine-readable part contains same information as human-readable part	If a non-human-readable encoding is used on the paper record, it SHALL contain the entirety of the human-readable information on the record	Agree with Requirement
2.6.3.6 Format for paper record non-human-readable data	Any non-human-readable information on the paper record SHALL be presented in a non-proprietary format.	Agree with Requirement
2.6.3.7 Linking the electronic CVR to the paper record	The paper record SHALL:	
2.6.3.7 Linking the electronic CVR to the paper record	a. Contain the paper record identifier; and	
2.6.3.7 Linking the electronic CVR to the paper record	b. Identify whether the paper record represents the ballot that was cast.	Recommend replacing "Identify" with "Validates"
2.7 Performance Monitoring		
2.7.1 Voting system and Network Status		
2.7.1.1 Network monitoring	The system server SHALL provide for system and network monitoring during the voting period.	More detail should be added as to what level of monitoring should be taking place. This could be as minimal as, "the light is green, the system is up".
2.7.1.2 Tool access	The system and network monitoring functionality SHALL only be accessible to authorized personnel from restricted consoles.	Agree with Requirement

Section	*Requirements*	*SLI Comments*
2.7.1.3 Tool privacy	System and network monitoring functionality SHALL NOT have the capability to compromise voter privacy or election integrity.	Agree with Requirement