STAR-Vote VVSG Gap Analysis

Summary of Notable Discrepancies

✓ *Compliant* ❗ *Non-Material Discrepancy* ✗ *Non-Compliant*

Discrepancy	*2005*	*2007*	*2012*	*Explanation of Gap*
Retrieval of human-readable ballot images	❗ 2.1.4 2.3.3 4.1.4	✓ n/a	❗ 2.1.4 2.4.4 4.1.4	In STAR-Vote it is possible to reconstruct individual human-readable electronic records during the risk-limiting audit process, and there are human-readable paper records available for inspection. However, at no time is it possible to simply access a collection of human-readable electronic ballot images. This is an intentional design intended to improve privacy guarantees.
Independent Safety Certification	✓ n/a	❗ 3.2.8	✓ n/a	While UL 60950-1 is applicable to COTS hardware, finding hardware which has been independently tested, or seeking independent testing may not be feasible given the use of COTS hardware.
Election Signature Keys	✓ n/a	✗ 5.1.4	✓ n/a	The requirement that device-specific Election Signature Keys be used to sign all election related data is supported by our design. However, those ESKs are created and signed by an Election Certification Authority which is unique to that election date. This allows for centralization of valid certificate creation which is necessary for enforcing device roles in the polling location network and protecting against the introduction of fraudulent records by 3rd parties.
Voting equipment status indicators required without the use of software	✓ n/a	❗ 5.2.3	✓ n/a	Under our interpretation, battery level indication provided by the operating system counts as "without the use of software." If this interpretation is incorrect, it is our opinion that no applicable COTS device currently on the market will meet the requirements for a power source charge indicator, a cabling connectivity indicator, or a communications status indicator as required
Securing audit logs through file access control	✓ n/a	✗ 5.4.4	❗ 2.1.5	Because STAR-Vote is designed to operate in a COTS hardware / operating system environment, it is designed to assume that we cannot effectively enforce access control policies to protect any data, and to still guarantee their integrity. We achieve this through a combination of hash chaining to provide tamper evidence, and massive duplication of all election-relevant log information across all devices in the polling location, making it exceptionally unlikely that any changes could be made uniformly to all devices without detection.
Anti-virus and Anti-malware software use	✓ n/a	✗ 5.5.4	✓ n/a	We explicitly disallow the introduction of antivirus or antimalware software into any element of the air-gapped system, since such software by design hooks into every facet of the operating system and processes, and therefore represents a substantial increase in the vulnerable attack surface of the voting system. Additionally, for such software to be useful an ability to connect to the internet would have to be provided to allow for "updates", introducing an unacceptable infection path into the system. Relying on the end-to-end encryption provides far more robust guarantees that the correct code has executed, and does so without introducing new vulnerabilities.
Ballot Counters	✗ 2.1.8	❗ 4.3.5	✗ 2.1.8	Requiring a physical ballot counter is impractical with COTS hardware, and its value would not be meaningful given STAR-Vote's challenge protocol. No ballots are officially "cast" until their paper record is placed in a ballot box, so no meaningful relationship will exist between the physical counters and the number of cast ballots. We believe the protections provided by our end-to-end encryption, hash chaining, and data redundancy provide far more useful and robust evidence of the number of ballots cast. A software ballot counter can be added if deemed necessary, but again will not have any relationship to the actual number of ballots cast.
Access to all hardware for testing prior to election	❗ 2.2.6	✓ n/a	❗ 2.2.6	Trustee computers, which are used during the tallying and decryption processes, will not be available to internal personnel once the election data has been created (probably several weeks before each election). It is certainly possible for internal personnel to test these devices before that point, however between then and the election each Trustee is responsible for the custody of their own Trustee computer. The distribution of these devices is used to prevent any small number of people from having the physical access necessary to violate the anonymity of votes in the electronic records.
Capability of every Tabulator to produce certain reports	✓ n/a	✓ n/a	❗ 2.4.4	"Tabulator" is no longer a meaningful concept in our system, as the data is combined and decrypted in a shared, distributed manner in which no one machine is the "tabulator". However, all required reports can be generated regarding the tabulation process, the tally is independently verifiable, and a complete log of each machine's contribution will be available for review.
Requirement for the use of sans-serif fonts	❗ 3.1.5	❗ 3.2.5	❗ 3.2.5	With modern high pixel density displays, there is growing evidence that serif fonts may be preferable both for ease of reading and for providing additional visual cues for limited vision voters. Given the high pixel density of displays available in typical COTS hardware today, we may permit serif fonts for use on very high pixel density displays.
Providing the same accessibility interfaces when reviewing the paper record that the voter had when making his selections	✓ 3.2.2	✓ n/a	❗ 3.2.2	Under our existing plan, one or more stations would be provided to read a paper record to a disabled voter through headphones, and optical magnifiers would be available to assist limited-vision voters. While this is not technically the same interface as required in the 2012 VVSG, we believe it more than fulfills its purpose.
Immunity to large power surges	✓ n/a	❗ 6.3.4	✓ n/a	The requirements around immunity to unusual voltage spikes will not be possible to meet using COTS hardware. However, the introduction of COTS surge protectors as part of the setup procedure would achieve the same end.
Various product marking / labelling and manufacturing log requirements	❗ 4.3.6	✗ 6.4	✗ 4.3.4 8.2	It is not possible to meet requirements around product marking, labelling, or manufacturing logging when the devices being used are COTS.
Requirement that independent processes be used for data storage	❗ 4.1.4	✓ n/a	✓ n/a	As a design decision, we will not be using independent processes for data storage. This decision is due to the increased attack surface provided by relying on interprocess communication. The goal of process-independent data storage is acheived through real-time massively redundant data replication across the network.

✓ *Compliant* ! *Non-Material Discrepancy* ✗ *Non-Compliant*

Discrepancy	*2005*	*2007*	*2012*	*Explanation of Gap*
Testing of all memory locations prior to use for storing election data	✗ 5.4.2	✓ n/a	✗ 5.4.2	Modern COTS non-volatile storage devices are too large for a systematic testing of all memory locations to be performed practically. As such to meet these requirements, we would have to pre-select locations on the drive to use and limit the size of potential data. This requirement would extend to volatile memory as well. Pre-selecting volatile or non-volatile memory locations is dispreferred as it makes attacks substantially easier than randomly assigned memory locations and, indeed, is very hard to acheive with a COTS operating system since most now include memory randomization inside their virtual memory system as a defense mechanism. Additionally, pre-selecting memory locations makes the system more vulnerable to small memory failures which are generally corrected by modern COTS systems simply by recognizing the failure and seamlessly using a different location. Limiting the size of data would be irrational given the space we have available in modern COTS systems and the detail its use permits in audit logs.
Confirmation of data transmission	! 6.2.7	✓ n/a	! 6.2.5	At various points it is required that the user be notified whenever a data transmission is successful. Due to our high-volume message passing system, there would be times when the user was receiving notifications several times per second, which is impractical and a usability nightmare. As a result, we prefer a "notify on failure" approach.
Requirement that all software to be used with the voting system be documented.	✗ 7.4.4	✓ n/a	✗ 7.4.4	Part of our logic in using a COTS operating system is the knowledge that newer versions of that operating system might become available, and newer or unanticipated hardware could be used. These two facts explicitly disallow the requirement that the system document all "software (such as operating systems and drivers) to be installed on the [...] voting system".
Certification of Cryptographic Modules	! 7.5.1	! 5.1.1	! 7.5.1	Certain cryptographic operations required by STAR-Vote are new enough to not have received NIST approval. Additionally, due to their state of the art nature, there may not be any FIPS 140-2 level 1 or higher validated cryptographic module implementing them. We will seek FIPS certification of our cryptography module, but cannot assure this at this time.
Ballot image randomization	✓ n/a	✓ n/a	! 7.8.3	Part of our system for detecting tamper evidence is a hash chain which, by design, enforces the ordering of ballot images. However, because our ballot images are not human readable and are never converted (or convertible) to a human-readable format, this does not endanger privacy.
Side-by-side comparison of the electronic summary and the paper record	✓ n/a	! 4.4.2	✓ n/a	We don't allow this both for usability and privacy reasons.
Physical tamper evidence mechanisms / hardware security	✓ 7.3	✗ 5.8 6.4.2	! 7.3	Embedded physical tamper evidence mechanisms are impractical to demand of COTS hardware. We firmly believe that the combination of procedural physical security measures -- including tamper-evident seals, tamper evident storage containers/bags, etc. -- end-to-end cryptography and a voter verified paper record provide the same level of confidence, and indeed an even more robust assurance of the system's correct operation, than embedded physical tamper evidence.
Providing the opportunity to void the ballot / paper record in the voting machine	! 7.9.2	✓ n/a	! 7.8.2	Under our system, the voting station does not know and, indeed, cannot know whether or not the voter intends to void the paper, nor can it mark the paper as void. Instead, our system treats a ballot as cast only once its paper record has been placed in a ballot box, and we permit voiding of the printed record by approaching a poll worker who marks the paper record void, and enables the voter to create a new ballot.

STAR-Vote VVSG 2005 (1.0) Detailed Gap Analysis

✓ *Compliant* ! *Non-Material Discrepancy* ✗ *Non-Compliant* [ ] *No Requirements*

Regarding	*Section*	*OK*	*Explanation of Gap / Notes*
Functional Requirements			
Overall System Capabilities	**2.1**		
Security	2.1.1	✓	
Accuracy	2.1.2	✓	
Error Recovery	2.1.3	✓	
Integrity	2.1.4	!	2.1.4 (l) requires that DREs have the capability to retrieve ballot images in a human-readable form. We meet this need through maintenance of a human-readable paper record placed in the ballot box. In STAR-Vote, one privacy protection mechanism is that it is impossible to reconstruct a readable ballot image from the electronic system prior to the Risk Limiting Audit.
System Audit	2.1.5	✓	
Election Management System	2.1.6	✓	
Vote Tabulating Program	2.1.7	✓	
Ballot Counter	2.1.8	✗	Requiring a physical ballot counter is impractical with COTS hardware, and its value would not be meaningful given STAR-Vote's challenge protocol. No ballots are officially "cast" until their paper record is placed in a ballot box, so no meaningful relationship will exist between the physical counters and the number of cast ballots. We believe the protections provided by our end-to-end encryption, hash chaining, and data redundancy provide far more useful and robust evidence. A software ballot counter can be added if deemed necessary.
Telecommunications	2.1.9	✓	
Data Retention	2.1.10	✓	
Pre-Voting Capabilities	**2.2**	✓	
Ballot Preparation	2.2.1	✓	
Election Programming	2.2.2	✓	
Ballot and Program Installation a ...	2.2.3	✓	
Readiness Testing	2.2.4	✓	
Verification at the Polling Place ...	2.2.5	✓	
Verification at the Central Locati ...	2.2.6	!	By design, Election Trustees' computers, which are involved in the tallying process, are not accessible to election officials and are custodied during the election by the various Trustees. This process makes it very difficult for any small group, including election officials, to materially affect the tally, and is robust to the loss, damage, or destruction of a small number of these devices (the exact number is configurable). This will limit the ability of election officials to engage in pre-election testing of this hardware as required in 2.2.6.
Voting Capabilities	**2.3**		
Opening the Polls	2.3.1	✓	
Activating the Ballot	2.3.2	✓	
Casting a Ballot	2.3.3	!	2.3.3.3 (q) requres access to plain-text ballot images. See 2.1.4 above.
Post-Voting Capabilities	**2.4**		
Closing the Polls	2.4.1	✓	
Consolidating Vote Data	2.4.2	✓	
Producing Reports	2.4.3	✓	
Broadcasting Results	2.4.4	✓	
Maintenance, Transportation, and ...	**2.5**	✓	
Usability and Accessibility Requirements			
Usability Requirements	3.1	✓	
Usability Testing	3.1.1	✓	
Functional Capabilities	3.1.2	✓	
Alternative Languages	3.1.3	✓	
Cognitive Issues	3.1.4	✓	
Visual Display Characteristics	3.1.5	!	With modern high pixel density displays, there is growing evidence that serif fonts may be preferable both for ease of reading and for providing additional visual cues for limited vision voters. Given the high pixel density of displays available in typical COTS hardware today, we may permit serif fonts for use on very high pixel density displays. Supporting reading of paper ballots for limited-vision voters is acheived through optical magnification.
Interaction Issues	3.1.6	✓	
Privacy	3.1.7	✓	
Accessibility Requirements	3.2	✓	
General	3.2.1	✓	
Vision	3.2.2	✓	
Dexterity	3.2.3	✓	
Mobility	3.2.4	✓	
Hearing	3.2.5	✓	
Speech	3.2.6	✓	
English Proficiency	3.2.7	✓	

✓ *Compliant* ! *Non-Material Discrepancy* ✗ *Non-Compliant* *[ ] No Requirements*

Regarding	*Section*	*OK*	*Explanation of Gap / Notes*
Cognition	3.2.8	✓	
Hardware Requirements			
Performance Requirements	**4.1**		
Accuracy Requirements	4.1.1	✓	
Environmental Requirements	4.1.2	✓	
Election Management System R ...	4.1.3	✓	
Vote Recording Requirements	4.1.4	!	As discussed previously, STAR-Vote does not allow the reconstruction of individual plaintext ballots from the electronic record, violating the DRE requirements in 4.1.4.3 (b) v. The paper record fulfills the purpose of this requirement. Furthermore, as a design decision, we will not be using independent processes for data storage as required for by 4.1.4.3 (b) iii. This decision is due to the increased attack surface provided by relying on interprocess communication. The goal of process-independent data storage is acheived through real-time massively redundant data replication across the network.
Paper-based Conversion Require ...	4.1.5	✓	
Tabulation Processing Requirem ...	4.1.6	✓	
Reporting Requirements	4.1.7	✓	
Vote Data Management Require ...	4.1.8	✓	
Physical Characteristics	**4.2**		
Size	4.2.1	✓	
Weight	4.2.2	✓	
Transport and Storage of Precin ...	4.2.3	✓	
Design, Construction, and Mainter ...	**4.3**		
Materials, Processes, and Parts ...	4.3.1	✓	
Durability	4.3.2	✓	
Reliability	4.3.3	✓	
Maintainability	4.3.4	✓	
Availability	4.3.5	✓	
Product Marking	4.3.6	!	The use of COTS hardware means that there will be no hardware available which meets the Product Marking requirements of section 4.3.6. This section's requirements could be met through the use of information added to the device by county personnel, or in the least preferred case, by manually affixing custom plates to the selected device's exterior. However, the use of COTS arguably makes the purpose of these required plates moot.
Workmanship	4.3.7	✓	
Safety	4.3.8	✓	
Software Requirements			
Scope	**5.1**		
Software Design and Coding Stand ...	**5.2**	✓	
Selection of Programming Langu ...	5.2.1	✓	
Software Integrity ...	5.2.2	✓	
Software Modularity and Progra ...	5.2.3	✓	
Control Constructs	5.2.4	✓	
Naming Conventions	5.2.5	✓	
Coding Conventions	5.2.6	✓	
Comment Conventions	5.2.7	✓	
Data and Document Retention	**5.3**	✓	
Audit Record Data	**5.4**	✓	
Pre-election Audit Records	5.4.1	✓	
System Readiness Audit Records ...	5.4.2	✗	5.4.2 (d) requires the explicit testing of all data paths and memory locations to be used prior to voting. No in-system process can successfully verify and audit, in any meaningful way, the integrity of data paths against malicious attackers which could mimic valid logs. As such, our defense of using trusted boot and signed executables offers superior evidence of validity. Additionally, memory randomization is a superior defense against malicious memory access as compared to testing of pre-defined memory locations, as it precludes the explicit targeting of pre-known memory locations by malicious code. The use of memory randomization precludes the effective testing of memory locations as required. Finally, as a matter of course, ballots which are known to be "test ballots" are meaningless from a security perspective, as a sophisticated attacker would detect that a given ballot was a "test" and withhold modification until real ballots were being cast.
In-process Audit Records	5.4.3	✓	
Vote Tally Data	5.4.4	✓	
Vote Secrecy on DRE Systems	**5.5**	✓	
Telecommunications Requirements			
Scope	**6.1**		
Design, Construction, and Mainter ...	**6.2**		
Accuracy	6.2.1	✓	
Durability	6.2.2	✓	
Reliability	6.2.3	✓	

✓ Compliant *! Non-Material Discrepancy* *✗ Non-Compliant* *[ ] No Requirements*

Regarding	*Section*	*OK*	*Explanation of Gap / Notes*
Maintainability	6.2.4	✓	
Availability	6.2.5	✓	
Integrity	6.2.6	n/a	
Confirmation	6.2.7	!	6.2.7 requires confirmation of successful or unsuccesful data transmission upon every occurance. Due to our model of massive data redundancy and constant message passing, meeting this requirement would lead to potentially hundreds of notifications of successful transmission per second in large polling locations. As such, we prefer a "notification of failure" model, with an implicit success assumption when no notification is provided. We believe our network protocol is robust enough to prevent undetected errors.
			Security Requirements
Scope	**7.1**		
Access Control	**7.2**		
General Access Control	7.2.1	✓	
Physical Security Measures	**7.3**	✓	
Polling Place Security	7.3.1	✓	
Central Count Location Security ...	7.3.2	✓	
Software Security	**7.4**		
Software and Firmware Installat ...	7.4.1	✓	
Protection Against Malicious Sof ...	7.4.2	✓	
Software Distribution and Setup ...	7.4.3	✓	
Software Distribution	7.4.4	✗	Part of our logic in using a COTS operating system is the knowledge that newer versions of that operating system might become available, and newer or unanticipated hardware could be used. These two facts explicitly disallow the requirement of 7.4.4 that the system document all "software (such as operating systems and drivers) to be installed on the [...] voting system".
Software Reference Information ...	7.4.5	✓	
Software Setup Validation	7.4.6	✓	
Telecommunications and Data Tra ...	**7.5**		
Maintaining Data Integrity	7.5.1	!	Certain cryptographic operations required by STAR-Vote are new enough to not have received NIST approval. We will seek FIPS certification of our cryptography module, but cannot assure this at this time.
Protection Against External Thre ...	7.5.2	✓	
Monitoring and Responding to E ...	7.5.3	✓	
Shared Operating Environment	7.5.4	✓	
Incomplete Election Returns	7.5.5	✓	
Use of Public Communication Net ...	7.6	n/a	
Wireless Communication	7.7	n/a	
Independent Verification Systems	**7.8**		
Overview	7.8.1	✓	
Basic Characteristics of IV Syster ...	7.8.2	✓	
Voter Verifiable Paper Audit Trail ...	7.9		
Display and Print a Paper Recorc ...	7.9.1	✓	
Approve or Void the Paper Reco ...	7.9.2	!	7.9.2 requires that the voting system itself provide a means of voiding the printed paper record. Under our system, the voting station does not know and, indeed, cannot know whether or not the voter intends to void the paper, nor can it mark the paper as void. Instead, our system treats a ballot as cast only once its paper record has been placed in a ballot box, and we permit voiding of the printed record by approaching a poll worker who marks the paper record void, and enables the voter to create a new ballot.
Electronic and Paper Record Stru ...	7.9.3	✓	
Equipment Security and Reliabil ...	7.9.4	✓	
Preserving Voter Privacy	7.9.5	✓	
VVPAT Usability	7.9.6	✓	Note: 7.9.6 (b) met via optical magnifiers
VVPAT Accessibility	7.9.7	✓	

STAR-Vote VVSG 2007 (2.0 Draft) Detailed Gap Analysis

✓ *Compliant* ! *Non-Material Discrepancy* ✗ *Non-Compliant* [ ] *No Requirements*

Regarding	*Section*	*OK*	*Explanation of Gap / Notes*
Usability, Accessibility, and Privacy Requirements			
Overview	**3.1**		
General Usability Requirements	**3.2**	✓	
Performance Requirements	3.2.1	✓	
Functional Capabilities	3.2.2	✓	
Privacy	3.2.3	✓	Note: The requirement for different font sizes on paper records will be met via optical magnifiers
Cognitive Issues	3.2.4	✓	
Perceptual Issues	3.2.5	!	With modern high pixel density displays, there is growing evidence that serif fonts may be preferable both for ease of reading and for providing additional visual cues for limited vision voters. Given the high pixel density of displays available in typical COTS hardware today, we may permit serif fonts for use on very high pixel density displays.
Interaction Issues	3.2.6	✓	
Alternative Languages	3.2.7	✓	
Usability for Poll Workers	3.2.8	!	3.2.8.2-A requires equipment be independently certified for compliance with the safety requirements of UL 60950-1. While UL 60950-1 is applicable to COTS hardware, finding hardware which has been independently tested, or seeking independent testing may not be feasible given the use of COTS hardware.
Accessibility Requirements	**3.3**	✓	
General	3.3.1	✓	Note: 3.3.1-E met via optical magnifiers and audio readers.
Low Vision	3.3.2	✓	
Blindness	3.3.3	✓	
Dexterity	3.3.4	✓	
Mobility	3.3.5	✓	
Hearing	3.3.6	✓	
Cognition	3.3.7	✓	
English Proficiency	3.3.8	✓	
Speech	3.3.9	✓	
Security and Audit Architecture			
Overview	**4.1**		
Requirements for Supporting Audi ...	**4.2**		
Pollbook Audit	4.2.1	✓	
Hand Audit of IVVR Record	4.2.2	✓	
Ballot Count and Vote Total Aud ...	4.2.3	✓	
Additional Behavior to Support ...	4.2.4	✓	
Electronic Records	**4.3**		
Records Produced by Voting Dev ...	4.3.1	✓	
Records Produced by Tabulators ...	4.3.2	✓	
Records Produced by the EMS	4.3.3	✓	
Digital Signature Verification	4.3.4	✓	
Ballot Counter	4.3.5	!	Requiring a physical ballot counter is impractical with COTS hardware, and its value would not be meaningful given STAR-Vote's challenge protocol. No ballots are officially "cast" until their paper record is placed in a ballot box, so no meaningful relationship will exist between the physical counters and the number of cast ballots. We believe the protections provided by our end-to-end encryption, hash chaining, and data redundancy provide far more useful and robust evidence of the number of ballots cast. A software ballot counter can be added if deemed necessary, but again will not have any relationship to the actual number of ballots cast.
Independent Voter-Verifiable Rec ...	4.4		
General Requirements	4.4.1	✓	
VVPAT	4.4.2	!	4.4.2.3-A requires that the voter have the opportunity to see the paper and electronic screens side by side, which we have explicitly disallowed to preserve privacy. Furthermore, 4.4.2.5-A requires that a printed record provide information sufficient to find its corresponding electronic record. While this is technically possible if Election Trustees participate, it is not possible under normal circumstances for auditors to make this link.
PCOS Systems	4.4.3	n/a	
General Security Requirements			
Cryptography	**5.1**		
General Cryptographic Impleme ...	5.1.1	!	Certain cryptographic operations required by STAR-Vote are new enough to not have received NIST approval. Additionally, due to their state of the art nature, there may not be any FIPS 140-2 level 1 or higher validated cryptographic module as required by 5.1.1-A. We will seek FIPS certification of our cryptography module, but cannot assure this at this time.
Digital Signatures for Election Re ...	5.1.2	✓	Note: Hardware TPMs will be required in COTS hardware to meet this requirement.
Key Management for Signature I ...	5.1.3	✓	Note: Hardware with an internal entropy source is necessary to meet this requirement. To my knowledge this would restrict hardware choices to Intel processors of the Ivy Bridge generation or later. Introduction of a 3rd party hardware entropy source is unrealistic and introduces additional design fragilities.

✓ Compliant   ! Non-Material Discrepancy   ✗ Non-Compliant   [ ] No Requirements

Regarding	*Section*	*OK*	*Explanation of Gap / Notes*
Election Signature Key	5.1.4	✗	The requirement that device-specific Election Signature Keys be used to sign all election related data is supported by our design. However, those ESKs are created and signed by an Election Certification Authority which is unique to that election date. This allows for centralization of valid certificate creation which is necessary for enforcing device roles in the polling location network and protecting against the introduction of fraudulent records by 3rd parties.
Setup Inspection	**5.2**		
Voting Device Software Inspecti ...	5.2.1	✓	
Voting Device Election Informati ...	5.2.2	✓	
Voting Equipment Properties Ins ...	5.2.3	!	Note: "Without the use of software" is ambiguous. Under our interpretation, battery level indication provided by the operating system counts as "without the use of software." If this interpretation is incorrect, it is our opinion that no applicable COTS device currently on the market will meet the requirements for a power source charge indicator, a cabling connectivity indicator, or a communications status indicator as required by 5.2.3-A, 5.2.3-B, and 5.2.3-D, respectively.
Software Installation	**5.3**	✓	
Access Control	**5.4**		
General Access Control	5.4.1	✓	
Access Control Identification	5.4.2	✓	
Access Control Authentication	5.4.3	✓	
Access Control Authorization	5.4.4	✗	Dual person control as required by 5.4.4-C falls outside the realm of COTS operating systems.
System Integrity Management	**5.5**		
Electronic Devices	5.5.1	✓	
Removable Media	5.5.2	✓	
Backup and Recovery	5.5.3	✓	
Malicious Software Protection	5.5.4	✗	We explicitly disallow the introduction of antivirus or antimalware software into any element of the air-gapped system, since such software by design hooks into every facet of the operating system and processes, and therefore represents a substantial increase in the vulnerable attack surface of the voting system. Additionally, for such software to be useful an ability to connect to the internet would have to be provided to allow for "updates", introducing an unacceptable infection path into the system. Relying on the end-to-end encryption provides far more robust guarantees that the correct code has executed, and does so without introducing new vulnerabilities.
Communication Security	**5.6**		
Physical Communication Securit ...	5.6.1	✓	
Data Transmission Security	5.6.2	✓	
Application Communication Sec ...	5.6.3	✓	
System Event Logging	**5.7**		
General System Event Logging	5.7.1	✓	
System Event Log Management ...	5.7.2	✓	
System Event Log Protection	5.7.3	✓	
Physical Security for Voting Device ...	**5.8**		
Unauthorized Physical Access	5.8.1	✗	Physical tamper evidence mechanisms are impractical to demand of COTS hardware. We continue to believe that the combination of end-to-end cryptography and a voter verified paper record provides substantially more robust assurance of the system's correct operation than costly and relatively less effective physical tamper evidence.
Physical Port and Access Least F ...	5.8.2	!	COTS hardware will in virtually all cases contain ports in excess of what is required for device testing and auditing. These ports can be physically disabled if necessary.
Voting Device Boundary Protect ...	5.8.3	✓	
Information Flow	5.8.4	!	5.8.4-B's requirement for port tamper evidence will be difficult to implement given the requirement for COTS hardware to rely on standard multi-function ports (such as USB) for providing accessibility peripheral connectivity. Given the design goal of making every device an accessible device, there must be at least one such open port on every device, which does not display tamper evidence when accessed.
Door Cover and Panel Security	5.8.5	✓	
Secure Ballot Box	5.8.6	✓	
Secure Physical Lock and Key	5.8.7	✓	
Physical Encasing Lock	5.8.8	n/a	
Power Supply	5.8.9	n/a	
General Core Requirements			
General Design Requirements	**6.1**	✓	
Voting Variations	**6.2**		
Hardware and Software Performa ...	**6.3**		
Reliability	6.3.1	✓	
Accuracy/Error Rate	6.3.2	✓	
Misfeed Rate	6.3.3	✓	
Electromagnetic Compatibility (E ...	6.3.4	!	The requirements around immunity to unusual voltage spikes will not be possible to meet using COTS hardware. However, the introduction of COTS surge protectors as part of the setup procedure would achieve the same end.
Electromagnetic Compatibility (E ...	6.3.5	✓	
Other Requirements	6.3.6	✓	

✓ *Compliant* ! *Non-Material Discrepancy* ✗ *Non-Compliant* [ ] *No Requirements*

Regarding	*Section*	*OK*	*Explanation of Gap / Notes*
Workmanship	**6.4**		
Software Engineering Practices ...	6.4.1		
Scope	6.4.1.1		
Selection of Programming Lar ...	6.4.1.2	✓	
Selection of General Coding C ...	6.4.1.3	✓	
Software Modularity and Proç ...	6.4.1.4	✓	
Structured Programming	6.4.1.5	✓	
Comments	6.4.1.6	✓	
Executable Code and Data Int ...	6.4.1.7	✓	
Error Checking	6.4.1.8	✓	
Recovery	6.4.1.9	✓	
Quality Assurance and Configura ...	6.4.2	✗	6.4.2.2 requires the use of model-specific tamper-resistant physical tags and manufacturing logs by unit. However, the use of COTS hardware effectively undermines the meaningfulness of these requirements.
General Build Quality	6.4.3	✓	
Durability	6.4.4	✓	
Maintainability	6.4.5	✗	6.4.5-C Requires certain nameplates and labels which simply will not exist on COTS hardware.
Temperature and Humidity	6.4.6	✓	
Equipment Transportation and S ...	6.4.7	✓	
Archival Requirements	**6.5**		
Archivalness of Media	6.5.1	✓	
Procedures Required for Correct ...	6.5.2	✓	
Period of Retention (Informative ...	6.5.3		
Integratability and Data Export/In ...	**6.6**	✓	
Procedures Required for Correct S ...	**6.7**	✓	
Requirements by Voting Activity			
Election Programming	**7.1**	✓	
Ballot Preparation, Formatting, an ...	**7.2**	✓	
Procedures Required for Correct ...	7.2.1	✓	
Equipment Setup for Security and ...	**7.3**		
Logic and Accuracy Testing	7.3.1	✓	
Opening Polls	**7.4**	✓	
Casting	**7.5**		
Issuance of Voting Credentials a ...	7.5.1	✓	
General Voting Functionality	7.5.2	✓	
Voting Variations	7.5.3	✓	
Recording Votes	7.5.4	✓	
Redundant Records	7.5.5	✓	
Respecting Limits	7.5.6	✓	
Procedures Required for Correct ...	7.5.7	✓	
Closing Polls	**7.6**	✓	
Procedures Required for Correct ...	7.6.1	✓	
Counting	**7.7**		
Integrity	7.7.1	✓	
Voting Variations	7.7.2	✓	
Ballot Separation	7.7.3	✓	
Misfed Ballots	7.7.4	n/a	
Accuracy	7.7.5	n/a	
Consolidation	7.7.6	✓	
Procedures Required for Correct ...	7.7.7	✓	
Reporting	**7.8**		
General Reporting Functionality ...	7.8.1	✓	
Audit, Status, and Readiness Rep ...	7.8.2	✓	
Vote Data Reports	7.8.3	✓	
Procedures Required for Correct ...	7.8.4	✓	

STAR-Vote VVSG 2012 (1.1 Draft) Detailed Gap Analysis

✓ *Compliant* ! *Non-Material Discrepancy* ✗ *Non-Compliant* [ ] *No Requirements*

Regarding	*Section*	*OK*	*Explanation of Gap / Notes*
Functional Requirements			
Overall System Capabilities	**2.1**		
Security	2.1.1	✓	
Accuracy	2.1.2	✓	
Error Recovery	2.1.3	✓	
Integrity	2.1.4	!	2.1.4 (i) requires that DREs have the capability to retrieve ballot images in a human-readable form. We meet this need through maintenance of a human-readable paper record placed in the ballot box. In STAR-Vote, one privacy protection mechanism is that it is impossible to reconstruct a readable ballot image from the electronic system prior to the Risk Limiting Audit.
System Audit	2.1.5	!	STAR-Vote ensures log integrity through massive duplication of election-relevant events between all computers in a polling location, and via the use of hash chains which provide tamper evidence. We believe this a substantial improvement over system-imposed file access controls as physical access to the device renders file access controls ineffective for even a moderately sophisticated attacker, whereas massive duplication and hash chaining provides genuine evidence that logs have not been modified.
Election Management System	2.1.6	✓	
Vote Tabulating Program	2.1.7	✓	
Ballot Counter	2.1.8	✗	Requiring a physical ballot counter is impractical with COTS hardware, and its value would not be meaningful given STAR-Vote's challenge protocol. No ballots are officially "cast" until their paper record is placed in a ballot box, so no meaningful relationship will exist between the physical counters and the number of cast ballots. We believe the protections provided by our end-to-end encryption, hash chaining, and data redundancy provide far more useful and robust evidence. A software ballot counter can be added if deemed necessary.
Telecommunications	2.1.9	✓	
Data Retention	2.1.10	✓	
Pre-Voting Capabilities	**2.2**	✓	
Ballot Preparation	2.2.1	✓	
Election Programming	2.2.2	✓	
Ballot and Program Installation a ...	2.2.3	✓	
Readiness Testing	2.2.4	✓	
Verification at the Polling Place ...	2.2.5	✓	
Verification at the Central Locati ...	2.2.6	!	By design, Election Trustees' computers, which are involved in the tallying process, are not accessible to election officials and are custodied during the election by the various Trustees. This process makes it very difficult for any small group, including election officials, to materially affect the tally, and is robust to the loss, damage, or destruction of a small number of these devices (the exact number is configurable). This will limit the ability of election officials to engage in pre-election testing of this hardware as required in 2.2.6.
Voting Capabilities	**2.3**		
Opening the Polls	2.3.1	✓	
Activating the Ballot	2.3.2	✓	
Casting a Ballot	2.3.3	✓	
Post-Voting Capabilities	**2.4**		
Closing the Polls	2.4.1	✓	
Consolidating Vote Data	2.4.2	✓	
Producing Reports	2.4.3	✓	
Electronic Reports	2.4.4	!	"Tabulator" is no longer a meaningful concept in our system, as the data is combined and decrypted in a shared, distributed manner in which no one machine is the "tabulator". However, all required reports can be generated regarding the tabulation process, the tally is independently verifiable, and a complete log of each machine's contribution will be available for review. Additionally, as stated above, STAR-Vote does not allow a mechanism for reconstructing individual ballot images electronically until the Risk Limiting Audit phase. Printed records exist for each cast ballot.
Election Night Reporting	2.4.5	✓	
Maintenance, Transportation, and ...	**2.5**	✓	
Usability and Accessibility Requirements			
General Usability Requirements ...	3.2	✓	
General Usability	3.2.1	✓	
Functional Capabilities	3.2.2	✓	Note: 3.2.2.1 (g) met through optical magnification.
Voter Privacy	3.2.3	✓	
Voter Instructions, Plain Language, ...	3.2.4	✓	
Visual Display Characteristics	3.2.5	!	With modern high pixel density displays, there is growing evidence that serif fonts may be preferable both for ease of reading and for providing additional visual cues for limited vision voters. Given the high pixel density of displays available in typical COTS hardware today, we may permit serif fonts for use on very high pixel density displays. Supporting reading of paper ballots for limited-vision voters is acheived through optical magnification.
Voter-Interface Interaction	3.2.6	✓	
Alternative Languages	3.2.7	✓	
Usability for Poll Workers	3.2.8	✓	
Accessibility Requirements	3.3	✓	

✓ *Compliant* ! *Non-Material Discrepancy* ✗ *Non-Compliant* [ ] *No Requirements*

Regarding	*Section*	*OK*	*Explanation of Gap / Notes*
General Accessibility	3.3.1	✓	Note: 3.3.1 (e) met through optical magnification.
Enhanced Visual Interfaces	3.3.2	✓	
Audio-Tactile Interfaces	3.3.3	✓	
Enhanced Input and Control Chara ...	3.3.4	✓	Note: 3.3.4 (b) met via 3.5 mm jack to USB accessory such as Swifty
Design for Mobility Aids	3.3.5	✓	
Enhanced Auditory Interfaces	3.3.6	✓	
Design in Support of Cognitive Disa ...	3.3.7	✓	
English Proficiency	3.3.8	✓	
Speech Not Required	3.3.9	✓	
Hardware Requirements			
Performance Requirements	**4.1**		
Accuracy Requirements	4.1.1	✓	
Environmental Requirements	4.1.2	✓	
Election Management System R ...	4.1.3	✓	
Vote Recording Requirements	4.1.4	!	As discussed previously, STAR-Vote does not allow the reconstruction of individual plaintext ballots from the electronic record, violating the DRE requirements in 4.1.4.3 (c). The paper record fulfills the purpose of this requirement. Furthermore, as a design decision, we will not be using independent processes for data storage as required for DREs by 4.1.4.3 (b) iii. This decision is due to the increased attack surface provided by relying on interprocess communication. The goal of process-independent data storage is acheived through real-time massively redundant data replication across the network.
Paper-based Conversion Require ...	4.1.5	✓	
Tabulation Processing Requirem ...	4.1.6	✓	
Reporting Requirements	4.1.7	✓	
Vote Data Management Require ...	4.1.8	✓	
Physical Characteristics	**4.2**		
Size	4.2.1	✓	
Weight	4.2.2	✓	
Transport and Storage of Precin ...	4.2.3	✓	
Design, Construction, and Mainter ...	**4.3**		
Materials, Processes, and Parts ...	4.3.1	✓	
Durability	4.3.2	✓	
Reliability	4.3.3	✓	
Product Marking	4.3.4	!	The use of COTS hardware means that there will be no hardware available which meet the Product Marking requirements of section 4.3.4. This section's requirements could be met through the use of information added to the device by county personnel, or in the least preferred case, by manually affixing custom plates to the selected device's exterior. However, the use of COTS arguably makes the purpose of these required plates moot.
Workmanship	4.3.5	✓	
Safety	4.3.6	✓	
Software Requirements			
Software Configuration	**5.1**	✓	
Software Design and Coding Stand ...	**5.2**	✓	
Scope	5.2.1		
Selection of Programming Langu ...	5.2.2	✓	
Selection of General Coding Star ...	5.2.3	✓	
Software Modularity and Progra ...	5.2.4	✓	
Structured Programming	5.2.5	✓	
Header Comments	5.2.6	✓	
Executable Code and Data Integ ...	5.2.7	✓	
Error Checking	5.2.8	✓	
Data and Document Retention	**5.3**	✓	
Audit Record Data	**5.4**	✓	
Pre-election Audit Records	5.4.1	✓	
System Readiness Audit Records ...	5.4.2	✗	5.4.2 (d) requires the explicit testing of all data paths and memory locations to be used prior to voting. No in-system process can successfully verify and audit, in any meaningful way, the integrity of data paths against malicious attackers which could mimic valid logs. As such, our defense of using trusted boot and signed executables offers superior evidence of validity. Additionally, memory randomization is a superior defense against malicious memory access as compared to testing of pre-defined memory locations, as it precludes the explicit targeting of pre-known memory locations by malicious code. The use of memory randomization precludes the effective testing of memory locations as required. Finally, as a matter of course, ballots which are known to be "test ballots" are meaningless from a security perspective as a sophisticated attacker would detect that a given ballot was a "test" and withhold modification until real ballots were being cast.
In-process Audit Records	5.4.3	✓	
Vote Tally Data	5.4.4	✓	

✓ *Compliant* ! *Non-Material Discrepancy* ✗ *Non-Compliant* [ ] *No Requirements*

Regarding	*Section*	*OK*	*Explanation of Gap / Notes*
Vote Secrecy on DRE and EBM Sys ...	**5.5**	✓	
Telecommunications Requirements			
Scope	**6.1**		
Design, Construction, and Mainter ...	**6.2**		
Accuracy	6.2.1	✓	
Durability	6.2.2	✓	
Reliability	6.2.3	✓	
Integrity	6.2.4	n/a	
Confirmation	6.2.5	!	6.2.5 requires confirmation of successful or unsucessful data transmission upon every occurance. Due to our model of massive data redundancy and constant message passing, meeting this requirement would lead to potentially hundreds of notifications of successful transmission per second in large polling locations. As such, we prefer a "notification of failure" model, with success assumed when no notification is provided. We believe our network protocol is robust enough to prevent undetected errors.
Security Requirements			
Scope	**7.1**		
Access Control	**7.2**		
General Access Control	7.2.1	✓	
Access Control Identification	7.2.2	✓	
Access Control Authentication	7.2.3	✓	
Access Control Authorization	7.2.4	✓	
Physical Security Measures	**7.3**	!	The use of COTS hardware potentially conflicts with hardware physical security measures prescribed by 7.3. It is our firm opinion that the presence of both a massively duplicated tamper-evident audit log and an independent paper vote record more than provide for the physical security which this section aims to acheive, and does so in a substantially more robust and meaningful
Polling Place Security	7.3.1	✓	
Central Count Location Security ...	7.3.2	✓	
Software Security	**7.4**		
Software and Firmware Installat ...	7.4.1	✓	
Protection Against Malicious Sof ...	7.4.2	✓	
Software Distribution and Setup ...	7.4.3	✓	
Software Distribution	7.4.4	✗	Part of our logic in using a COTS operating system is the knowledge that newer versions of that operating system might become available, and newer or unanticipated hardware could be used. These two facts explicitly disallow the requirement of 7.4.4 that the system document all "software (such as operating systems and drivers) to be installed on the [...] voting system".
Software Reference Information ...	7.4.5	✓	
Software Setup Validation	7.4.6	✓	
Telecommunications and Data Tra ...	**7.5**		
Maintaining Data Integrity	7.5.1	!	Certain cryptographic operations required by STAR-Vote are new enough to not have received NIST approval. Additionally, due to their state of the art nature, there may not be any FIPS 140-2 level 1 or higher validated cryptographic module as required by 7.5.1 (b). We will seek FIPS certification of our cryptography module, but cannot assure this at this time.
Protection Against External Thre ...	7.5.2	✓	
Monitoring and Responding to E ...	7.5.3	✓	
Shared Operating Environment	7.5.4	✓	
Election Returns	7.5.5	✓	
Use of Public Communications Ne ...	**7.6**	n/a	
Wireless Communications	**7.7**	n/a	
Voter Verifiable Paper Audit Trail ...	**7.8**		
Display and Print a Paper Recorc ...	7.8.1	✓	
Approve or Void the Paper Reco ...	7.8.2	!	7.8.2 requires that the voting system itself provide a means of voiding the printed paper record. Under our system, the voting station does not know and, indeed, cannot know whether or not the voter intends to void the paper, nor can it mark the paper as void. Instead, our system treats a ballot as cast only once its paper record has been placed in a ballot box, and we permit voiding of the printed record by approaching a poll worker who marks the paper record void, and enables the voter to create a new ballot.
Electronic and Paper Record Stru ...	7.8.3	!	7.8.3 (a) requires randomization of the ordering of ballot images. We explicitly disallow ballot image randomization due to the use of hash chaining to provide tamper evidence. The goal of anonymity protection afforded by ballot randomization is instead guaranteed in a more meaningful manner in our system through encryption of vote tallies, and through the use of a distributed mixnet in our ultimate decryption process that makes it impossible for any one individual (or even a small group of colluding individuals) to trace specific plaintext votes back to a specific voter.
Equipment Security and Reliabil ...	7.8.4	✓	
Preserving Voter Privacy	7.8.5	✓	
VVPAT Usability	7.8.6	✓	Note: 7.8.6 (b) met via optical magnifiers
VVPAT Accessibility	7.8.7	✓	
Quality Assurance and Configuration Management			
Standards-based Framework for Qu ...	8.1	✓	
Configuration Management Requir ...	8.2	✗	8.2 requires the use of model-specific tamper-resistant physical tags and manufacturing logs by unit. However, the use of COTS hardware effectively undermines the meaningfulness of these requirements.