True E2E V Systems – Metrics

CATEGORY	FACTORS	REMOTEGRITY	HELIOS	RIES - NETHERLAND
User Trust	1. Whom or what does the voter need to trust that			
	1.1. An authentic blank ballot from LEO is delivered to the voter's computer/device. Must voter trust			
	a) Voter's own computer/device?[12]	No	Yes	No
	b) The Internet and the ISPs -- of voter's internet service & election office?[13]	No	Yes	No
	c) Local election officials?	Yes	No	No
	d) Computer equipment or software at the LEO, such as a server, network, +/or the VS software	No	Yes	Yes
	e) Some third party, such as a printing company or other vendor, e.g., for delivery of printed or the creation of coded electronic ballots, which are accurately mapped to the candidates' names?	Yes	Yes	Yes
	1.2. Voter's ballot contains the choices that voter had marked at the time he/she attempts to return the marked/voted ballot to the LEO, specifically that no change has occurred between the voter's marking the ballot & the LEO's receipt of the marked ballot. Must voter trust			
	a) Voter's own computer/device? [14]	No	Yes	Yes
	b) The Internet and the ISPs -- of voter's internet service & election office?	No	Yes	Yes
	c) The Internet (for transmission of the	No	Yes	Yes

[12] In other words, can malware on the voter's computer change the voter's ballot such that the voter cannot detect changes (an inauthentic ballot) & these are changes are also undetectable at the election office?

[13] For instance, does the voting system send authentic ballots that are not susceptible to change by personnel or automated malware at the ISP or at other intermediate internet transmittal "hops"?

[14] In other words, could malware change the voter's ballot choices such that the changes are undetectable at the election office? This might occur in some systems if malware on the voter's computer can covertly modify the vote choices before the ballot is transmitted to the LEO. If the voter must independently check—i.e., "audit" the ballot that the LEO has received

	voted ballot)?			
	d) The local election officials personally?	No	No	No
	e) Computer equipment at the LEO, such as a server, network, +/or the VS software.	No	Yes	Yes
	f) A vendor that administers the election for LEO/outsourcing	No	Unclear	Unclear
	1.3. Voter's marked ballot is correctly recorded in the tabulation database at election office - Must voter trust-			
	a) Voter's own computer/device? [15]	No	No	Yes
	b) The Internet and the ISPs -- of voter's internet service & election office?	No	No	Yes
	c) The Internet (for transmission of the voted ballot)?	No	Yes	Yes
	d) The local election officials personally?	No	No	Yes
	e) Computer equipment at the LEO, such as a server, network, +/or the VS software.	No	Yes	Yes
	f) A vendor that administers the election for LEO/outsourcing	No	Unclear	Unclear
	g) VS electronic "Bulletin Board"	No	Yes	No
Voter Anonymity	1. Is it possible to associate or connect the identity of a voter with a particular cast ballot or vote, at the point of			
	a. Voter's transmittal of a marked ballot to the election office, over the internet?	No	Unclear	Yes
	b. At LEO, the recording of vote choices in the database?	No	No	No
	c. Reporting of final results?	No	Yes	No
Security	*1. Was the system tested for security vulnerabilities by security experts?* Were:	Yes	No	Yes
	1.1. ***Network security vulnerabilities*** identified?	Unclear	Unclear[16]	Unclear

[15] In other words, could malware change the voter's ballot choices such that the changes are undetectable at the election office? This might occur in some systems if malware on the voter's computer can covertly modify the vote choices before the ballot is transmitted to the LEO. If the voter must independently check—i.e., "audit" the ballot that the LEO has received.

[16] Due to the lack of security testing for the Helios System by a reliable third party, the ability to establish the existence or lack of existence of any vulnerabilities has been compromised. In light of these developments, all scenarios that may address any vulnerabilities have been labelled as "unclear" until testing has occurred.

	a) If yes, how many vulnerabilities?	Unclear	Unclear	Unclear
	b) Were the vulnerabilities fixed?	Unclear	Unclear	Unclear
	c) If not, are they planned to be fixed?	Unclear	Unclear	Unclear
	d) Have the vulnerability fixes been independently reviewed by qualified security experts?	Unclear	Unclear	Unclear
	1.2. ***Application security vulnerabilities*** identified?	Yes	Unclear	Unclear
	a) If yes, how many vulnerabilities?	Unclear	Unclear	Unclear
	b) Were the vulnerabilities fixed?	Yes	Unclear	Unclear
	c) If not are they planned to be fixed?	N/A	Unclear	Unclear
	d) Have the vulnerability fixes been certified by security experts?	Unclear	Unclear	Unclear
	2. Were the results of such testing published internally or publically?	Unclear	Unclear	Yes
	3. Is the system resilient to:			
	a. Client side malware?	Yes	No	No
	b. Server side malware?	Yes	No	Unclear
	4. Does the system allow detecting changes to the integrity of the votes during:			
	a. Casting of ballots?	Yes	Yes	Yes
	b. Recording of casted ballots?	Yes	Yes	Yes
	c. Tallying the recorded ballots?	Yes	Yes	Yes
	5. Can the changes to integrity detected, be corrected in the system?	Yes	Yes	Yes
	5.1. Is the recovery process Automated or manual?	Manual	Manual	Automated and Manual
	6. Is there a defined Recovery Time Objective[17] associated with the system?	Unclear	Unclear	Unclear
	7. Is there a defined Recovery Point Objective[18] associated with the system?	Unclear	Unclear	Unclear
	8. Does the voting system incorporate any technical or administrative measure to deter, prevent, detect, and defend against Voter Coercion?	No	No	No

[17] The recovery time objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity

[18] Recovery point objective is the maximum tolerable period in which data might be lost from an IT service due to a major incident

	9. Does the voting system incorporate any technical or administrative measure to deter, prevent, detect, and defend against LEO coercion?	No	No	Unclear
Auditability	1. Does the system produce a voter-verifiable, durable, tamper-evident artifact (abbreviated "V V-D-TEA")?[19]	Yes	Yes	Yes
	2. Can any additions, deletions, or substitutions to the voter's ballot selections (votes) be detected, using the V V-D-TEA records?	Yes	Yes	No
	3. Can the results of the election contests (races and issues) be reconstructed (recounted) independently of using the voting system's software, simply by using the V V-D-TEA records?[20]	Yes	Yes	No
	4. Does the system require additional audit checks, for instance by using digital signatures and hashes?	Yes	Yes	Yes
	5. Does the voting system support the auditing of:			
	a) Number of blank ballots sent to voters	Yes	N/A	Yes
	b) Number of voted ballots received from voters	Yes	Yes	Yes
	c) Verifiability of cast as recorded	Yes	Yes	Unclear
	d) Verifiability of tallied as cast	Yes	Yes	Yes
	6. Does the auditability design of the voting system require via hard-coded [nondiscretionary, within range of reasonability] logs of operators' interaction with:			
	a) Blank ballots generator/database	Yes	Unclear	Yes
	b) Voted ballots collection system/database	Yes	Unclear	Yes
	c) Cast ballots storing system/database	Yes	Unclear	Unclear
	d) Cast ballots tallies	Yes	Unclear	Unclear
	e) Cast ballots reports	Yes	Unclear	Unclear
	f) System failures, malfunctions and other threats or attacks on operation of	Yes	Unclear	Yes

[19] Noted voting system auditing expert Dr. Phillip Stark recommended this set of attributes that we have abbreviated "V V-D-TEA."

[20] This question asks for whether the system can be described as producing a voting record and potential for election results that are "software independent." See Rivest & Stark, and Stark & Wagner (cites)

	the voting system, as well as other infrastructure components			
	7. Are these audit logs protected from administrative or operator modifications (insider threat)?	Yes	Yes	Unclear
	8. Are these audit logs protected against operations (e.g., system crashes) or attacks which could lead to data corruption or loss?	Yes	Yes	Unclear
	9. Does the audit system maintain voter anonymity at all times?	Yes	Yes	No
Testing & Development	1. Has the system received reliability testing or any other testing specified by the Voluntary Voting System Guidelines (VVSG)?	No	No	Unclear
	2. Has the system been submitted for certification under the EAC voting system process?	No	No	No
	3. Has the system received open-ended vulnerability testing, as recommended by the EAC's Technical Guidelines Development Committee?	No	No	Unclear
	4. Has the system undergone any other independent testing, not by the internal developers but by a qualified independent organization or set of individuals?	No	No	Yes
	5. Have the developers announced any planned independent testing?	No	No	No
	6. Is the system currently or planned to be deployed for:			
	a) Public Government election?	No	No	Yes
	b) Private, nonprofit, labor union election?	Yes	Yes	No
Usability	1. Has a usability study been conducted by qualified usability assessors and published for public or scholarly access?	No	Yes	Yes
	2. If yes, did the study report deficiencies in the system with regard to usability by voters, specifically regarding			
	a) Comprehension & success in ***marking*** of ballot?	Unclear	Yes	Unclear
	b) Comprehension & success in ***casting*** of ballot?	Unclear	Yes	Unclear
	c) Comprehension & success in ***verifying*** of ballot?	Unclear	Yes	Unclear
	3. Did the study report usability deficiencies in the system with regard to election official set up of the election?	Unclear	No	Unclear

Accessibility	1. Has an accessibility study been conducted by qualified accessibility assessors, published by public or scholarly access?	No	No	Unclear
	2. Is the system designed for persons with physical impairments that may affect voting?			
	a) Blind	Unclear	No	No
	b) Deaf	Unclear	Yes	No
	c) Multiple impairments	Unclear	Unclear	No

Score Assignment

(High – 5, Medium – 3, Low – 0)

Area	Score Assignment to responses
User Trust	No = 5, Yes = 3, Unclear =0
Voter Anonymity	No = 5, Yes = 0, Unclear =0
Security	Yes = 5, No = 0, Unclear = 0
Auditability	Yes = 5, No =0, Unclear = 0
Testing & Development	Yes = 5, No =0, Unclear = 0
Usability	Yes = 5, No =0, Unclear = 0
Accessibility	Yes = 5, No =0, Unclear = 0

Systems Score Table

Area	Max Possible Score	Remotegrity	Helios	RIES
User Trust	90	86	58	58
Voter Anonymity	15	15	5	10
Security	110	50	25	30
Auditability	85	85	50	40
Testing & Development	35	5	5	10
Usability	25	0	20	5
Accessibility	20	5	5	0

Scoring Qualification Statement:

The systems evaluated in this report have been analyzed using publicly disclosed documents and have not been subjected to an independent product evaluation. The scoring for these systems (above) is not weighted, but that weighting would likely be useful for producing a final set of valid metrics. The scores are not indicative of a certain outcome or overall judgment but are simply a visual representation of the narratives presented earlier in this report.