

VVSG Comments for Part 1; Sections 5 through 5.3. This does not include an analysis of the testing and evaluation processes and their adequacy to these requirements.

Comments developed by Tom Caddy

#	PARA ID	PARAGRAPH TITLE	VVSG STATEMENT	COMMENT	SUGGESTION
1	5.1.1-A	Cryptographic Module	Cryptographic functionality <i>SHALL</i> be implemented in a FIPS 140-2 validated cryptographic module operating in FIPS mode.	It should not be allowed to have a non FIPS mode. Non-FIPS modes allow for vulnerabilities in the modules that will degrade trust of integrity, crypto keys and processes. The statement about having a FIPS mode of operation is meaningless because if it did not have a FIPS mode it could not be validated.	Add sentence: The cryptographic module used in voting systems shall not have a non-FIPS mode of operation.
2	5.1.1-B	Cryptographic Strength	The specified strength should be sufficient for several decades	Table 4 of 800-57 Part 1 says 112 bits of strength should be ok through 2030 then 128 bits will be required. This is a guide that is not fixed if some new threat appears. This is actually a maximum of two decades.	Opt 1) Delete sentence. Opt 2) Modify sentence to indicate until 2030.
3	5.1.1-B	Cryptographic Strength	This requirement is not intended to forbid all incidental use of non-approved algorithms by OS software or standardized network security protocols.	This is a built in waiver that is not consistent with FIPS 140-2 compliant cryptography. This will allow vendors to build in insecure protocols and process that are not necessary at this time. There are enough approved methods to implement any objective in the elections arena.	Delete paragraph The statements allowing a tolerable amount of flexibility are built into the FIPS 140-2 standard.
4	5.1.2	Digital signatures for election records	The purpose of signing election records is to authenticate them and prevent their subsequent alteration	Digital Signatures do not <i>prevent</i> subsequent alteration, they do enable a very high confidence that the record was altered.	Modify sentence: Enable the detection of a modified or altered record.
5	5.1.2	Digital signatures for election records	This makes it more difficult to falsify election records so that a careful audit would not detect evidence of the alteration or would not detect that election fraud had occurred	This sentence is incorrect since Digital Signatures cannot <i>prevent</i> alteration.	Modify sentence: This makes it difficult to falsify election records without creating evidence of the alteration that has a high assurance of detecting the change.

#	PARA ID	PARAGRAPH TITLE	VVSG STATEMENT	COMMENT	SUGGESTION
6	5.1.2	Digital signatures for election records	A separate hardware <i>Signature Module (SM)</i> protects the private signature keys and the signature process should the election system software be compromised.	Specific words likely to be miss interpreted: Separate (to what degree is it separated, is separate in conflict with permanent in next sentence) Hardware (What constitutes hardware, a chip with firmware or a pc or process with external memory. It is correct it needs to be a hardware (level 3) Cryptomodule).	Modify sentence: A cryptographic module implemented as a FIPS 140-2 Level 3 certified <i>Signature Module (SM)</i> protects the private signature keys and the signature process and therefore the critical “cast vote record” CVR.
7	5.1.2	Digital signatures for election records	The module is “embedded in” (permanently attached to) the voting device to make it difficult to substitute another module.	Specific words likely to be miss interpreted: Embedded (it may not be necessary for the crypto module to be classified as embedded by the CMVP) Permanent (If key management and signature verification processes are architected correctly, a substituted signature module would be detected and flagged). To make the SM permanent would be not maintainable.	Modify sentence: The module is an integral component of the voting device CVR signatures will also be verified outside the device with the public key to detect SM substitution.
8	5.1.2-A	Digital Signature generation requirements	Digital signatures used to sign election records <i>SHALL</i> be generated in an embedded hardware Signature Module (SM).	Specific words likely to be miss interpreted: Election Records: (Section 5 is basically the only area where the term election records is used. This needs to be defined because elections have a lot of records that are not part of these described processes. Is this really CVR’s? If so replace Election records with CVR’s). Embedded (it may not be necessary for the crypto module to be classified as embedded by the CMVP)	Modify Sentence: Digital signatures used to sign CVR’s <i>SHALL</i> be generated in a Signature Module (SM) integral to the Programmed Device.
9	5.1.2-A	Digital Signature generation requirements	This makes it more difficult to create spurious election records.	Replace term “create spurious”.	Modify Sentence: This makes it more difficult to modify or substitute CVR’s.
10	5.1.2-B	Signature Module	Programmed devices that sign election records <i>SHALL</i> contain a hardware cryptographic module, the Signature Module (SM), that is capable of generating and	Programmed devices that sign election records, this sounds like it is possible to have a programmed device that does not sign election records? If so this is a big loophole. It seems like Programmed	Vote capturing devices shall sign CVR’s and shall be implemented in a FIPS 140-2 certified cryptographic module, that is capable of both generating and

#	PARA ID	PARAGRAPH TITLE	VVSG STATEMENT	COMMENT	SUGGESTION
			protecting signature key pairs and generating digital signatures.	devices maybe more appropriately termed vote capturing device per the glossary.	protecting signature key pairs and also generating and (verifying ?) digital signatures.
11	5.1.2-B	Signature Module	For the purpose of this requirement a “hardware” cryptographic module means a distinct electronic device , typically a preprogrammed, dedicated microcomputer that holds keying material and performs cryptographic operations.		
12	5.1.2-B	Signature Module	Although today this might typically be a single chip, soldered onto a larger motherboard, it is not the intent of this guideline to preclude higher levels of integration. It is expected that future voting devices may integrate the SM onto the same die as the rest of the voting device, as long as the SM is clearly physically and logically separated on the die from the rest of the voting device so that there is a distinct cryptographic module boundary, and there is no way for the rest of the device to access signature private keys except through the defined cryptographic module interface.	<p>Although a good idea.</p> <p>This is not currently a certifiable under FIPS 140-2 and is not planned to be an option under 140-3 which is expected to be implemented next year.</p> <p>Current technology does not enable a reasonable method to prove adequate separation and independent trust with a single die.</p> <p>This would be more difficult for most labs then evaluating software for vulnerabilities</p>	Delete sentence.
13	5.1.2-B	Signature Module	Signature verification and other cryptographic operations need not be implemented in hardware, but may also be implemented on the embedded signature module if desired.	Clarification suggested.	Modify Sentence: Signature verification is not required as a service of the SM but is an optional service.

#	PARA ID	PARAGRAPH TITLE	VVSG STATEMENT	COMMENT	SUGGESTION
14	5.1.2-B.1	Non-replaceable embedded Signature Module (SM)	if there is a motherboard, the SM would typically be soldered to the motherboard of the voting device.	This specified feature adds no security to the system, anyone with very little skill and time can remove a soldered in component.	
15	5.1.2-B.1	Non-replaceable embedded Signature Module (SM)	If the core of the voting device is contained on a single chip computer, the module would be a distinct, integral, but independent processor on that chip that does not share logic or memory with other functions.	Partial chips are not certifiable as 140-2 modules at this time. See number 12 above.	
16	5.1.2-B.1	Signature Module Validation level	Signature Modules <i>SHALL</i> be validated under FIPS 140-2 with FIPS 140 level 2 overall security and FIPS 140 level 3 physical security.	It seems that the SM should be validated to level 3 across the board. The only reason not to is identity authentication which seems to be appropriate.	Modify to indicate Level 3 overall
17	5.1.2-B.1	Signature Module Validation level	FIPS 140 level 3 physical security requires tamper resistance.	Level 3 physical security is not best defined as tamper resistance. If it is a multichip module then it requires tamper detection and response plus tamper evidence.	Modify description.
18	5.1.3-C	Device Certificate storage	Device Certificates <i>SHALL</i> be stored permanently in the SM and be readable on demand by the programmed device.	1) Numbering format changes from previous paragraph. 5.1.3.1-B 2) Permanently is an awkward word here. What if the device is sent back to the factory, the Private key should have been erased which would make the DSK certificate unusable.	Modify sentence: Indicate a service shall be available to read/export the certificate. Also indicate the key pair and certificate are persistent throughout the service life of that serial number device, or similar concept.
19	5.1.3-E	Device Signature Key Protection	Once the key is installed in the SM it cannot be changed or read out	A Key installed in the SM is in conflict with the requirement statement that the DSK is created and exists only inside the crypto module.	Modify discussion to be consistent with requirement.
20	5.1.4-A	Election Signature Key (ESK) Generation	Signature Modules <i>SHALL</i> internally generate election signature key-pairs (ESK) using an integral nondeterministic random bit	Non Deterministic RNG's are not acceptable on their own for FIPS 140-2.	Modify sentence to indicate FIPS 140-2 compliant and do not specify NDRNG or DRNG.

#	PARA ID	PARAGRAPH TITLE	VVSG STATEMENT	COMMENT	SUGGESTION
			generator.		
21	5.1.4-D	Election Signature Key use counter		Add discussion paragraph	
22	5.1.4-E	Election Key Closeout	When the election is complete, the ESK private key is destroyed so that election records cannot be forged at a later time.	<p>1) The key is erased so that another record cannot legitimately be added after the counting is complete. "Forged" is the wrong context.</p> <p>2) This is a critical function that disables a mode of operation. These type actions should require two independent actions to be executed.</p>	Modify sentence: Replace forged with added
23	5.1.4-F	Election Key Closeout record	The format of the Election Key Closeout Record is not specified and might be either a signed XML object or it might, potentially, use another signed format such as the ASN.1 Cryptographic Message Syntax.	It is not appropriate to provide examples as they will cause confusion. It will become a program issue if it is not one of the examples and who decides which examples are ok.	Modify sentence: Delete all after "not specified"
24	5.2.1	Voting device Software inspection	Software definition	This should really apply to all "LOGIC" in the system, whether Software, Firmware, GateArrays, ROM etc. The FIPS 140-2 program has separate cases for some of these and ignores others, I believe that will become an issue with Voting equipment. Yet those other logic control "software" mechanisms are not addressed.	
25	5.2.1.1-B.1	EMS Software identification verification log	EMSs and other programmed devices that identify and authenticate individuals also <i>SHALL</i> record identifying information of the individual and role that performed the inspection.	<p>1) No discussion paragraph!</p> <p>2) The title talks about software identification but the requirement talks about individual authentication. One or the other is wrong.</p> <p>3) 5.2.1 is about voting devices somehow this jumps to EMS's</p>	
26	5.2.1.2-B			No discussion paragraph.	
27	5.2.1.2-	EMS Software	EMSs and other programmed	1) No discussion paragraph	

#	PARA ID	PARAGRAPH TITLE	VVSG STATEMENT	COMMENT	SUGGESTION
	B.1	integrity verification log	devices that identify and authenticate individuals also <i>SHALL</i> record identifying information of the individual and role that performed the inspection.	2) This is exactly the same requirement as 5.2.1.1-B.1 3) The title talks about software identification but the requirement talks about individual authentication. One or the other is wrong. 4) 5.2.1 is about voting devices somehow this jumps to EMS's	
28	5.2.2-B.1	Voting Device, election information value inspection log		Numbering incorrect is 5.2.1.2-B.1 should be 5.2.2-B	
29	5.2.2-B.1	EMS, election information value inspection log		Numbering incorrect is 5.2.1.2-B.1 should be 5.2.2-B.1	
30	5.2.3-H	Voting Device, property inspection log		Numbering incorrect is 5.2.1.2-H should be 5.2.3-H	
31	5.2.3-H.1	EMS, property inspection log		Numbering incorrect is 5.2.1.2-H.1 should be 5.2.3-H.1	
32	5.3-G	Programmed device, software installation logging		Numbering incorrect is 5.2.1.2-G should be 5.3-G	
33	5.3-G.1	EMS, Vote equipment property inspection log		Numbering incorrect is 5.2.1.2-G.1 should be 5.3-G.1	
34	5.3-J	Programmed Device, configuration file access logging		Numbering incorrect is 5.2.1.2-J should be 5.3-J	
35	5.3-J.1	EMS configuration file access logging		Numbering incorrect is 5.2.1.2-J.1 should be 5.3-J.1	