

March 21, 2019

Attendees

John Wack
John Dziurlaj
Amy Cohen
Katy Owens Hubler

Status Updates

- There probably won't be a TGDC meeting until sometime in June but EAC wants to see what requirements look like before then.
- John: working to make VVSG more about the devices and how they operate, and the documentation. Then there's a whole series of other requirements about how systems are supposed to be tested and other things that are required by the EAC certification process. Currently that's all mixed together in the VVSG. Separating them would make them more flexible and less confusing for test labs.
- Today looking at the documentation requirements.
- John took requirements in VVSG 1.1 and 2007 VVSG that was updated in 2012 as a base. Changed some of those requirements. Purpose today is to get brief thoughts on things that stand out, should be changed or added.

Discussion

- 3.1-A.2: System Overview documentation, functional diagram
 - This is like a "quick start guide" that doesn't go into detail but explains overall what the components are, where they came from, how to plug it in, etc. It also provides context so that when you do go into more specific documentation you have a general overview in your mind.
- 3.1-A.2: System Overview, system description
 - It's possible there's too much in here. Hoping to do a meeting with test labs and manufacturers to talk it over.
- 3.1-A-4: System overview, traceability of procured software
 - Cybersecurity group is also working on supply chain management issue. Requirements like this one will likely be superseded by cybersecurity group requirements or supply chain requirements from DHS.
- 3.1-B.1: System performance
 - Limits, constraints, associated benchmarks with specific performance.
- Security requirements are interspersed with other requirements rather than grouped together. It would be good to have them tagged or some sort of database to see these more easily.
- 3.1-C.2 System security, system event logging
 - Previously there was a feeling that we should have a lexicon common to all devices – for example if a ballot is cast the event code should be the same. We eventually moved away from that. "Casting" a ballot may mean different things on different devices and could be constraining in different ways.
 - Currently language may need to be tweaked:
Manufacturers must provide user documentation that:
 - describes system event logging capabilities and usage

- publicly available and free of charge, fully documents the log format information
- 3.1-C.3 Audit
 - Cybersecurity might have broken this out into a separate section.
 - Voting systems should at the minimum provide a way to audit, but maybe the requirements shouldn't go into specifics on that.
- 3.1-D Software installation
 - How to install, how to you know when it's installed, how is the software identified, where did it come from.
 - Some of these may be functional requirements in disguise.
- 3.1-E Setup inspection process
 - How do you know the system is set up properly and how can you monitor its operations to make sure it's functioning correctly – for example logic and accuracy testing would fall under this, though it isn't called out specifically.
- 3.1-K Training manual
 - Does this belong and does it need to be called out?
 - No comments
- 3.1-L Specification of common format usage
 - If you implemented a CDF you need to show how it was used. It's possible for the CDFs to be misused, so this describes ways to validate it.
- Amy: if you pull things out of these requirements, where would they go?
 - John: probably in the certification manuals. Can't speak for the EAC but these may need to be reorganized, a process in place for modifying the requirements as circumstances change, but they would go over to the EAC documents that would still be public.
 - John: also going through to make sure that the requirements are applicable for a "voting device" rather than a "voting system" to allow for component testing if necessary.
- Working on packaging it so that it can be explained to the TGDC and others. Part of the meetings with the boards would be to identify any areas where there is potential disagreement.
- John managed the VVSG development process in 2007 and realized that what we should have done is allow people the opportunity to look at it as it's being developed, so that we get to a place where people generally agree with it so that it isn't voted down in the end.
- We don't really have any major conflicts in the interoperability work. The manufacturers aren't always keen about having CDFs required, so there will probably additional feedback and possible reorganization on those.

Next Steps

- These documents will be on GitHub for review.