From: Traci Mapps
To: votingsystemguidelines@eac.gov
Subject: UOCAVA Pilot Program Testing Requirements - Comments
Date: 04/15/2010 11:58 AM

To Whom it May Concern,

SysTest is excited about new UOCAVA Pilot Program and appreciates the opportunity to submit comments in regards to the testing requirements. Please see our comments below and feel free to contact me with any questions that you may have.

With regard to section 1.2, UOCAVA Remote Electronic Voting System Scope, while the first paragraph discusses that the UOCAVA systems tie multiple different systems and jurisdiction together in order to present the appropriate ballot style to the involved voters, and as such need access to the involved systems EMS and voter registration databases, there does not seem to be any requirements that speak to how this will be done. It seems that this is the crux of the UOCAVA project, but it does not have any detail as to how the importation of different systems, different implementations of the same voting system, different sizes/types of ballot styles, how the printout of physical "ballots" will be done such that each governing jurisdiction can/will make use of them, etc. These are probably issues that go beyond the Okaloosa project, where they probably only had one unique system and didn't need to be concerned with incorporating multiple vendors data schemes into one(?) comprehensive scheme. In our work, we have encountered this situation between just two vendors attempting to integrate their systems, and it was not a simple task. We believe that this, in particular needs additional thought and guidance.

Test Method, while appendix A does define Inspection, there are no definitions for Functional or Vulnerability. Guidance in these areas may be helpful.

It seems the VSTLs should have the authority to write up documentation discrepancies found, even where the manufacturer is the official test entity. Therefore, when the VSTL encounters discrepancies while preparing to test or during testing of the system, they will be documented and can be considered by the EAC.

The use of algorithms may not be rigorous enough. Perhaps this should be NIST (or FIPS)-approved implementations. The concern being that an approved algorithm can still be implemented incorrectly/poorly.

- 5.3.1.3 Cryptography/Use NIST-approved cryptography for communications
- 5.5.1.3 Virtual private networks (FIPS)

These are not necessarily voting system requirements. Perhaps these should be in the Testing and Certification Program Manual as there would not be methods to test these.

- 5.9.2.5 Penetration testing team establishment
- 5.9.2.6 Penetration testing level of effort-test plan
- 5.9.2.7 Penetration testing level of effort

As the VSTL is dependent on these for creation of the test plan, perhaps this requirement should be under the domain of the VSTL.

- 8.1.1.1.1 TDP/Identify full system configuration
- 8.1.1.1.2 TDP/Required content for pilot certification

Test Entity: Manufacturer

Best Regards,

Traci Mapps
Director of Operations
SysTest Labs Incorporated
216 16th Street, Suite 700
Denver, Colorado 80202
☎ Phone: 303.575.6881 x155
🖷 Fax: 303.575.6882
✉ Email: tmapps@systes.com
Web: www.systest.com