Testimony of

Mark Skall

Before the

U.S. Election Assistance Commission

“UOCAVA Pilot Program Testing Requirements”

April 8, 2010

Introduction

Chair Davidson, Commissioners Hillman, Beach, and assembled members of the public, thank you for the opportunity to testify today.

I will discuss the pilot program testing requirements for the Uniformed and Overseas Citizen Absentee Voting Act, better known as UOCAVA.

Background

As we all know, the present system for UOCAVA voters is deficient due to the fact that mail transit time and unreliable delivery pose significant barriers for many UOCAVA citizens, arguably resulting in the disenfranchisement of many of our uniformed and overseas voters. Consequently, several States have passed legislation enabling them to conduct electronic voting projects for UOCAVA voters, beginning with the 2010 elections. This legislation necessitated the need for developing requirements for UOCAVA systems, which would then be used to test and certify these systems. Since the existing voluntary voting system guidelines did not envision remote voting technologies, those requirements were not sufficient to test UOCAVA systems. Thus, in order to support the States in conducting electronic voting projects for UOCAVA voters, the EAC convened a UOCAVA Working Group to consider how to adapt the EAC's Testing and Certification Program to accommodate UOCAVA pilot systems. It was concluded that two products were needed: 1) a modified set of system testing requirements; and 2) a revised testing and certification process. It was further decided that the source material for the UOCAVA testing requirements would be extracted from existing standards and guidelines, when feasible. These standards and guidelines include the Voluntary Voting System Guideline (VVSG) 1.0, 1.1 and 2.0, the Voting Over the Internet (VOI) project, SERVE and Okaloosa project requirements and NIST products, including Federal Information Processing Standards (FIPS) and NIST Special Publications. The Working Group was well aware that some of the source requirements needed to be modified for the new UOCAVA Requirements document. Furthermore, if a requirement, not available in the source documents, was needed, it would be developed by the Working Group.

Differences between UOCAVA and General Election Testing and Certification

A typical test campaign to test voting systems for the general election is very comprehensive and thorough and takes a long time to complete. Testing time has ranged from six months to two years. The long testing time is a necessary outgrowth of two factors: 1) the inclusion of many detailed requirements in the voluntary voting system guidelines; and 2) the need for Voting System Test Laboratories (VSTL), with the oversight of the EAC, to comprehensibly test each and every requirement.

The UOCAVA pilot program, however, had its own set of criteria if it was going to be successful. Since pilot programs are small in scale and duration, testing for these systems needed to be much quicker and less expensive than for conventional systems in the general election. However, since real votes are cast and counted in these pilot systems, thoroughness and rigor cannot be sacrificed. Thoroughness and rigor are assured by including sufficient requirements to allow testers and voters to have confidence that the resulting voting systems are reliable, secure and usable.

Consequently, it was decided to include all appropriate requirements and *not to exclude* any requirement just because it would make the system less costly and faster to test. Instead, the mechanism used by the Working Group, to dramatically decrease the time and cost of testing, was to assign the testing of some requirements to the manufacturer of the pilot UOCAVA system. Thus, testing of requirements would be divided between the VSTL and the manufacturer. The testing of critical requirements was assigned to the VSTL while the testing of non-critical requirements was assigned to the manufacturer of these pilot UOCAVA systems. After all, manufacturers need to comprehensibly test their systems during system development. Thus, they would be able to re-use many of the tests they had already developed, resulting in less costly and faster certification testing. By employing this dual-testing strategy the knowledge, expertise and experience of the manufacturer could be leveraged.

Risks in Manufacturer Testing

There are, of course, risks in allowing manufacturers to test their own systems to determine whether they conform to many of the requirements in this document. There is obviously an incentive for manufacturers to save time by testing requirements less comprehensively than would ordinarily be done by VSTLs and perhaps, even more importantly, to allow their own systems to pass tests for requirements that more objective testers, like VSTLs, would fail them on. To mitigate this possibility, it was determined that stringent oversight by the EAC is necessary. This oversight, plus other factors, will help to ensure that manufacturer testing will be done accurately and comprehensively. First, the manufacturer will legally attest to the accuracy of the test results submitted to the EAC. Second, the EAC will review the test results and associated documentation, from the manufacturer (as well as from the VSTL) and make a determination that all requirements have been appropriately tested and that the test results are acceptable. Third, the EAC will conduct audits of manufacturer testing to ensure its adequacy. Any determination that a manufacturer has not conducted testing properly, will result in loss of certification. This combination of legal attestations and physical audits will provide us with sufficient confidence in the manufacturer testing, while enabling dramatically faster and less costly testing.

Equivalent Configurations

Under the current EAC certification program (prior to this document), the scope of certification is very specific and extends only to the exact voting system configuration tested. Any modification to the system, not authorized by the EAC, will void the certificate. However, in the UOCAVA testing and certification process, since the systems being certified are COTS systems, flexibility is needed to accommodate routine and expected changes to these COTS systems. Thus, in UOCAVA testing, the concept of "equivalent configuration" was introduced. In UOCAVA, an equivalent configuration is a voting system configuration that differs in some minor way from the tested voting system and has been attested by the manufacturer to perform identically to the tested baseline configuration. The requirements document enumerates very specific instances of changes that are allowed to be made without resulting in re-testing. In providing for equivalent configurations, the UOCAVA Requirements document provides the needed flexibility to accommodate routine and expected changes to these COTS systems. Without this flexibility, UOCAVA systems would have to be continually re-tested due to many routine changes, such as operating system security patches, which are typically applied every few days.

UOCAVA Pilot Program Testing Requirements

Developing a standard or guideline, in any environment, is a difficult task. It entails coalescing many different representatives of different constituencies and getting them to agree on specific requirements that then have to be carefully worded to accomplish the collective intent. The standard or guideline then needs to not only clearly delineate the set of requirements, but also provide enough explanatory text so that different readers of the standard can discern what is being required.   This is especially difficult in the world of elections where the degree of public scrutiny is so great that the readers of the standard are many and varied. In developing standards for elections, the challenge is to supplement very technical information with non-technical descriptions so that many different constituencies can understand the document.

The UOCAVA Pilot Program Testing Requirements document faced even greater challenges. First, the composition of the EAC UOCAVA Working Group had to be decided, including the organizations that would participate, as well as deciding which individuals representing those organizations to invite. Decisions needed to be made with respect to the platform architecture that would be tested by these requirements. Next, crucial determinations on what requirements were to be part of each section needed to be made, as well as decisions as to which entity, the VSTL or the manufacturer, would be assigned the responsibility to test each and every requirement. Furthermore, since this document was intended to be used for the 2010 elections, there was a very specific, and incredibly short, timeframe in which to develop this unique document. Lastly, the document had to read as if it were written by one person. It needed to be internally consistent, uniform and homogeneous. This was an especially difficult task since these requirements had been gleaned from many different sources and had been written by Working Group members with widely diverse backgrounds.

In spite of all of these obstacles, the UOCAVA Pilot Program Testing Requirements is an excellent set of requirements. The requirements are well-specified, clear and concise. They are comprehensive, yet not overly-constraining. Each and every requirement references not only the test entity that is going to test that requirement but this document is also is the first voting standard or guideline to describe the test method to be used. The UOCAVA requirements document is also the first voting standard or guideline to incorporate comprehensive requirements for penetration testing. Penetration testing, similar to open ended vulnerability testing, involves an active analysis of the voting system to attempt to discover potential vulnerabilities.

Conclusion

The UOCAVA Requirements document is a seminal voting system guideline. It addresses needed functionality for UOCAVA systems and does this in a unique and ground-breaking manner. It introduces new and innovative ways to specify requirements and to test and certify UOCAVA systems. The UOCAVA Requirements document is only a first step. It assumes the kiosk model, in which the voting platform is provided by the election jurisdiction. We will eventually need to migrate to the model where the voter uses his or her own computer to vote. The Working Group was well aware of this and attempted to define requirements so that, as much as possible, they could be carried over to support the other model. The TGDC has been tasked to consider the full range of remote voting architectures, including instances where voters can use their own personal computer for voting. The pilot testing requirements document will be turned over to the TGDC as a starting point for their research and deliberations. As stated earlier, the UOCAVA Requirements document is only a first step – but it is an essential first step.

Thank you for the opportunity to testify. I will be happy to answer any questions you may have.