From: [redacted]
To: votingsystemguidelines@eac.gov
Subject: UOCAVA Pilot Program Testing Requirements
Date: 04/30/2010 03:46 PM

Dear EAC:

I am writing to comment on the UOCAVA Pilot Program Testing Requirements.

I am a senior software consultant, formerly at Digital Equipment Corporation. I have been programming for over 25 years, and have been involved in election technology since 2005. My web site is www.CountedAsCast.com.

To start, it needs to be stated that voting over a network is not by itself "highly secure", at least with respect to the purpose for which this is intended, federal elections. What is at risk here is the very government of the United States. This far surpasses the security needs of a bank or oil company. The risk increases when "The systems will require linkages to the local Election Management System" (pg 8). This give the opportunity for anybody with access anywhere on the network to manipulate elections in the various counties, both by changing who can vote, and by changing how they voted. Any direct electronic linkage to the voter registration systems, and to the election management systems entails a substantial risk that is being glossed over by those pushing these kinds of systems.

The fundamental principle of security at this level is - trust nobody. That would include - trust no network, and no software. This would include networks operated by the government, and COTS software. These systems are far too vast and complex, they have too many open attack vectors, to permit the assumption that they are secure. Yet, given what is at stake, that is the reckless assumption that is being made here.

The best way to deal with security risks is redundancy. To its credit, the possibility of redundancy exists within the proposed system, because it includes a paper record. Yet, amazingly, a full hand count of all the paper records is not a requirement of this system. That makes it a non-starter. Any and all remote voting systems should require a full hand count of all paper voting records, at the voting location. After the paper records have been sent, there should be a thorough spot check by the local election officials of those same ballots. This is what a bank does when it ships money. Any at-risk system needs double checks, aka redundancy.

I remind the EAC that California (1) forbids the direct connection of the Election Management System to any external network, and (2) requires a 100% hand count of all votes cast on DREs. These are not radical requirements, they are the minimal requirements for any voting system that could approach being called "secure". The EAC should be enforcing the same requirements on any system being proposed for use in federal elections. A failure to do so is putting the government of the United States at unnecessary risk, and it must be corrected.

Thank you for your attention.

Yours,

Jim Soper

Senior Software Consultant
www.CountedAsCast.com