From:	W. Parish test
Reply To:	W. Parish test
To:	votingsystemguidelines@eac.gov
Subject:	comments on UOCAVA testing
Date:	04/23/2010 02:37 PM
Attachments:	UOCAVA Pilot Program Testing Requirements.doc

Skip Parrish
[redacted]

UOCAVA Pilot Program Testing Requirements - EAC request for comments.

UOCAVA is dependant on online communications for US Citizens and Military persons wishing to conduct voting functions from foreign locations. The test program is void in any discussion, procedures, applications and other necessary security issues inherent in the transmission of confidential and voter specific data concerning these functions.

Two issues addressed in these comments:

1. Lack of any system for checking and maintenance of authentic genuine COTS parts, software, and other related executable programs used in communications and on voting devices. .

2. No testing and or specifications on transport layer of specific voter information used to obtain voting privileges, absentee ballots, or other voting related online functions for Military persons. (Information Security)

Registration in most States for voters requires personal information such as Name, Address, Date of Birth, Social Security Number, Current Address, Previous Address, Drivers License or other ID, and signature, for the request of Absentee Ballots most States require Name, Address , Previous Address, DOB, and Signature. Given this information is specific to a single voter and in the case of the military valuable to the enemy it is considered classified in most cases with regard to troop deployment.

The testing requirements fail to test and or address the type of information security to be used by the military or suppliers to protect the transport layer of communications, path, custody of data, and other communication elements common to messages across foreign countries. The Military has the sole responsibility for the protection of its troops and thus the final decision on transport of data across foreign countries and battlefields as to information security shall rest on the cyber security offices of the Secretary of Defense. With this issue not addressed by this testing and requirements and without direct liaison with the uniformed military cyber security the program can not be given a high probability of success even in pilot testing.

A program with liaison of the cyber security departments of the Department of Defense is an imperative at this point to complete this program for military voters to use this system and pilot tests. The mission of the FVAP is not information security of troops, and this function can not be left to NIST (National Institute of Testing) who does not have the final reasonability of information security for the military. (Specialize branches of the US Military have this responsibility)

UOCAVA is also dependant on hardware and software of current suppliers and remote software / hardware located in foreign countries. The method and path of the data in getting to and from users is key to the program and the security of the program chain of custody. This report contains NO measures or process for the certification of hardware and software as to original US manufacture and use. The program will use more hardware and software in its mission that is considered COTS than actual software and hardware that have been tested under this program as the data travels across nation states. Unlike aircraft certification of parts and original equipment this program has no certification facility

for genuine tested parts or original equipment. COTS parts are a key element in the workings of this program in communication of votes and voter functions and counterfeit hardware and software constructed for specific missions is a part of our work environment.

The United States Government has had experience with counterfeit parts know as COTS in the past, as when the Federal Bureau of Investigation purchased Cisco Routers a US company for communications only to find after use that the y contained software modifications through foreign manufacture to divert copies of communications to foreign governments.

The UOCAVA program testing metrics need to verify and certify original manufacture and US manufacture of tested parts and communication security paths for all operations that involve the Military, this plan has no facility to do this thus the chain of custody can not be assured or carry an acceptable level of protection for its users as well as protect the Military specific troop information.

The UOCAVA program technology needs to comply with Regulations with regard to hardware and software used for military voters to protect the information security of data this testing and plan has no facility for that. In addition the pilot programs such as Operation Bravo in the past have employed foreign companies to provide path of communications, server farms, staff, and security encription with out regard to this regulation or approval of the US State Department/ Military as to method and practice. This program needs to comply with information security suitable to the needs of the Military where it involves military voting using specific troop information in electronic form.

It is suggested to the EAC/NIST and FVAP that electronic collection of information is accessable, efficient and ubiquious in Nation States so much so that it can n ot be compared to the loss of information on hard copy documents sent through the mail. Further electronic messages all have an orgion ation and termination point in the signal and thus add information on the user n ot possiable with regular hard copy mail. Any specifications for the intended activity contained in UOCAVA must include and address these critical problems for our Military voters and the protection of operations.