School of Computer and Information Sciences
University of South Alabama
Mobile, Alabama 36688
251.460.6390

May 15, 2009

Lynden Armstrong, Chief Clerk
United States Senate
Committee on Rules and Administration
Russell Office Building
305 Russell Senate Office Building
Washington, DC 20510

Dear Chief Clerk Armstrong,

Attached please find written testimony for the May 13 meeting of the U. S. Senate Committee on Rules and Administration to hear testimony regarding voting problems facing military members and their families. Thank you for this opportunity to present written testimony.

Please do not hesitate to contact me if you have questions.

Sincerely,

Alec Yasinsac, Dean

WRITTEN TESTIMONY OF ALEC YASINSAC, PH.D.
SCHOOL OF COMPUTER AND INFORMATION SCIENCES
THE UNIVERSITY OF SOUTH ALABAMA
PREPARED FOR THE UNITED STATES SENATE COMMITTEE ON RULES AND ADMINISTRATION MEETING TO HEAR TESTIMONY ON PROBLEMS FOR MILITARY AND OVERSEAS VOTERS
MAY 13TH, 2009

Thank you for the opportunity to provide testimony to this meeting. My name is Alec Yasinsac. I am Professor and Dean of the School of Computer and Information Sciences at the University of South Alabama. I have significant voting system experience, having conducted numerous government sponsored voting system security reviews and have over thirty years experience in computers and communication systems. I am also a retired Marine that voted absentee for most of my twenty years of service.

The problems that face military voters and their families are vast and have gone on for far too long. Efforts to date to chip away at the corners of the problem typify a modification to an old adage:

A-little-bit-better is the enemy of good-enough.

Military members are disproportionately disenfranchised in alarming numbers and we must commit the resources, and will, to make the necessary changes to eliminate this disparity.

This testimony first identifies four specific voting problems for military members and their families that are stationed overseas:

(1) The present system does not provide sufficient time for military members and their families to vote.

(2) Mistakes by military members and their families are markedly unforgiving as compared to other voters.

(3) Vote by Mail is inherently insecure for military members and their families.

(4) There are unnecessary barriers to military support for the voting process.

It then provides recommendations that can lead to timely, reliable voting for military members and their families stationed overseas.

The present system does not provide sufficient time for military members and their families to vote.

In the past five months, the Overseas Vote Foundation, National Institute of Standards and Technology, and Pew Charitable Trusts released reports on Military and Overseas Voting. The U. S. Elections Assistance Commission (EAC) commissioned a study on this topic in 2007, as did the U. S. General Accounting Office (GAO).

It is encouraging that the topic is receiving significant attention, as is well demonstrated by this hearing. This attention is long overdue.

Maybe the most telling of all the facts that emerged from these reports is that the *good news* is that:

> *[1]31 of our 50 states provide enough time for their deployed military and overseas residents to vote.*

Yes, this is the good news. Taken from the report released by Pew Trusts on January 6 of this year, we know that nineteen of our fifty states do not provide enough time for military/overseas voters to successfully cast their ballot. This illustrates just how pervasive the challenges are to enabling military members and their family to cast their ballots.

It is instructive to examine what it means in the PEW Report for overseas voters to have "enough" time. From the same report:

> *The average time required for overseas voters to cast their ballots in those states is 29 days*

This means that in those states that provide enough time to vote, overseas voters begin the voting process twenty nine days before election day, effectively

[1] Pew Trusts, "No Time to Vote", January 6, 2009, http://www.pewtrusts.org/news_room_detail.aspx?id=47924

imposing a 29-day penalty on overseas and military voters.

A canonical UOCAVA voting process may apply some form of the following serial steps:

(1) Voter requests an official absentee ballot request form

(2) The local jurisdiction processes the request and puts the absentee ballot request form in the mail to the voter

(3) The mail system delivers a blank absentee ballot request form to the voter

(4) The voter fills out the absentee ballot request and puts it in the mail to their election jurisdiction

(5) The mail system delivers the completed absentee ballot request to the voter's jurisdiction

(6) The jurisdiction processes the request, authenticates the voter, resolves any discrepancies in the voter's record, and selects the proper ballot. When the ballot is ready, the jurisdiction puts the ballot in the mail. Note that the ballot cannot be selected until after the jurisdiction finalizes the ballots, which may be fairly close to election day.

(7) The mail system delivers the blank ballot to the voter

(8) The voter receives the blank ballot, marks the ballot, and places the marked ballot in the mail to be returned to their jurisdiction

(9) The mail system delivers the marked ballot to the jurisdiction

(10) The jurisdiction processes the ballot and incorporates it into the vote tally on election day

Each of these serial steps takes time and is dependent on human processes. An error or delay in any step can cause the cycle to fail resulting in disenfranchisement.

Moreover, while some states allow unregistered voters to combine their registration with their absentee ballot request, some states may prefix the following steps into the process for unregistered UOCAVA voters:

(0.1) Voter requests an official registration request form

(0.2) The local jurisdiction processes the request and puts the blank registration form in the mail

(0.3) The mail system delivers a blank registration form to the voter

(0.4) The voter fills out the registration form and puts it in the mail to their jurisdiction

(0.5) The mail system delivers the completed registration form to the jurisdiction

(0.6) The local jurisdiction processes the request, authenticates the voter, resolves any discrepancies in the voter's record, and enters them into the voter rolls

This prospective sixteen step process, with six mail-dependent steps, does not represent the worst case, which includes additional iterations necessitated by errors. It is certainly possible to reduce the time required for military members and their families to vote by reducing the number of steps in this process, and all states exercise some form of step reduction. Pushing information and materials, rather than waiting for requests, can reduce the time required, but often depends on stable location information, which is not possible with many military voters.

Moreover, chipping away at the number of required steps cannot remove the inherent delays in international mail. Military members deserve to be confident that their ballots will be counted on election day and that

their votes will be included in the first reported count. Election materials transported through international mail cannot offer that assurance.

Mistakes by military members and their families are unforgiving compared to other voters.

An often overlooked aspect of this issue is that the voting experience for military voters is much less rich than for their polling place counterparts. For example, depending on the state from which they hail and other details of the situation, military voters may not be able to:

- Change their mind
- Employ routine voting error checks
- Fix mistakes
- Reliably track their ballot
- Stop in to vote on their way to work
- Register on election day
- Change residence close to election day

Think of the simplest of restrictions: if while marking their ballot a military voter errantly selects a candidate, the only means to make a correction may be to request a replacement ballot[2] and it is unlikely that a replacement ballot could arrive in time to complete the process in most cases. Additionally, if after they

[2] Some states offer VBM voters procedures to correct mistakes

mail their ballot they gain additional information about the candidates, e.g. by watching a televised debate, they are unlikely to be able to change their mind because of the inherent delivery delays.

Certainly, any one of the listed issues can be overcome, but when combined, their result is devastating to this voting group. The collective impediments are highlighted by the contrast between the percentage of requested absentee ballots returned among the general voting population (86%) and those from overseas/military voters (27%) (also from the Pew Report).

This is an apples-to-apples comparison. Voters that go to the trouble of requesting an absentee ballot are serious about voting. They are willing to devote the effort necessary to cast their ballot. Military voters are being disenfranchised in large numbers.

Many of these problems are related to the time required to transport materials between military members and their voting jurisdiction. Materials transported through international mail cannot offer the services needed to support voting for military members and their families.

Vote by Mail (VBM) is inherently insecure for military members and their families.

The VBM system that the preponderance of military voters and their families use does not support the fundamental voting system requirements of coercion resistance, vote-sale resistance, verifiable privacy, nor are they auditable. In many cases, if military members residing overseas are able to detect that their VBM ballot was not delivered, they are unable to attain and send a replacement ballot in time to be counted.

There are many ways that VBM ballots offer limited reliability and accountability.

Lost mail. The mail system is designed to deliver a large volume of mail in a short time. It is not generally designed to track each item, so, as many of us have experienced ourselves, mailed items are routinely lost.

Because of its design that does not establish a rigorous chain of custody, any approach that employs regular mail, marked ballot delivery is not auditable. Mail can be lost with no ability to find lost items, or in some cases, even to detect their loss.

Voter errors. VBM procedures are inherently complex and error prone. We found little broadly applicable historical data on this topic, but in the 2008 election

in Minnesota approximately 4.2% of all VBM ballots were rejected (approximately 12,000[3] of 288,000[4]) due to procedural errors by voters. Common errors include failure to sign, signing in the wrong place, and improper packaging (e.g. husband and wife bundling two absentee ballots in the same envelope).

This 4.2% vote loss percentage does not include ballot marking errors that may have been prevented or corrected at the polling place, so the overall vote loss/error rate is likely substantially higher than 4.2%, while in-precinct ballot rejection is likely near zero percent.

Election official errors. Inherently complex VBM procedures are also difficult for temporary elections officials, even those who routinely process VBM ballots, to understand and follow. In Minnesota, at least 13% of the rejected absentee ballots were rejected in error[5]. The actual percentage of erroneously rejected ballots may be higher, because there may still be erroneously rejected ballots that have not been detected. In one Minnesota county[6], after the senate contest was certified and reviewed, another, further review revealed that 20% (30 of 150) of the thrice-

[3] Startribune.com, "Senate recount: Pendulum swings to Franken", By MIKE KASZUBA and CURT BROWN, December 3, 2008
[4] http://www.sos.state.mn.us/docs/postpercanvassingreport1117250p.pdf
[5] http://www.startribune.com/opinion/editorials/36194339.html?elr=KArks7PYDiaK7DUqyE5D7UiD3aPc:_Yyc:aUU
[6] http://www.startribune.com/politics/national/senate/39314392.html?elr=KArks7PYDiaK7DUvDE7aL_V_BD77:DiiUiD3aPc:_Yyc:aUU

reviewed rejected ballots had been erroneously rejected by local elections officials "...who misunderstood state law or mishandled ballot applications".

Administering VBM ballots is an inherently complex process and significant errors are certain to occur.

Duplicated ballots. Many jurisdictions require elections officials to duplicate damaged or difficult-to-read VBM ballots. This creates a significant opportunity for mishap, as in the Minnesota senate race where the Wall Street Journal[7] suggests that duplicates may have been counted twice in several precincts.

> *But it appears some officials may have failed to mark ballots as duplicates, which are now being counted in addition to the originals. This helps explain why more than 25 precincts now have more ballots than voters who signed in to vote.*

Vote Attribution. Voter privacy is commonly seen as the voters' ability to cast their ballot without anyone being able to know their selections. VBM is inherently susceptible to violations of this minimal privacy interpretation since each VBM ballot must be bound to the voter's identity in order to ensure one-person, one-vote. Elections officials institute procedures to protect voter privacy, but the inherent vulnerability

[7] http://online.wsj.com/article/SB123111967642552909.html

still exists for every VBM ballot. VBM does not protect against vote attribution and is susceptible to widespread fraud.

There are unnecessary barriers to military support for the voting process.

There are two specific barriers that limit the ability to resolve problems for military voters. First, there is an unfounded aversion toward directly involving the military establishment in the voting process. Like dental, medical, and postal services, voting services must be provided as an essential service to military members and their families.

Presently, the military's additional duty Voting Assistance Officer provides voting information to military members and their families, but there is little operational voting service provided. The types of voting services that should be provided for military members and their families include, but are not limited to:

- Early voting centers
- Absentee ballot collection centers
- Electronic ballot delivery systems
- Network applications to support voting services

I have heard some express a hesitancy to formally involve the military establishment in any aspect of the

voting process due to the risk of coercion. This concern is unfounded in empirical evidence and Chapter 29, Title 18 of the U. S. Code deals specifically with that concern. Military members and their families will continue to be disproportionately disenfranchised until the military adopts voting as an essential service and commits the correspondingly appropriate resources to provide that service.

Second, there is significant inertia to bind voting advances for military members and their families to similar gains for non-military overseas voters. This binding discounts the many fundamental differences in the two groups, including significant information security capabilities enabled by identity and oversight requirements for military members and their families. The two most obvious enabling distinctions are the military identification card that military members and their families carry and the access to military networks enjoyed on military bases.

While UOCAVA governs both military voters and non-military overseas citizens, it does not preclude leveraging resources that are specific to any subgroup of covered citizens.

In order to correct more than one hundred years of military disenfranchisement, we must leverage every

advantage that military administration provides with no artificial or preconceived limitations.

Recommendations that can lead to timely, reliable voting for military members and their families stationed overseas.

The greatest single opportunity to fix voting for military members stationed overseas is to eliminate the multi-day transmission delay for election materials between the voter and their voting jurisdiction. Virtually all of the problems that overseas military members face become imminently solvable if the transmission time shrinks from days to minutes or hours.

The Overseas Vote Foundation[8] (OVF) is a champion of using the Internet to provide an electronic conduit between overseas voters and their voting jurisdiction for many election materials. The progress they have made in the past few years is remarkable. Since their efforts and capabilities are well known, the rest of testimony focuses on a critical area that OVF has not pursued: electronic delivery of marked ballots.

[8] http://www.overseasvotefoundation.org/

The frustration of military voters is exemplified by the following note from a military member recorded in the January 2009 report from OVF:

> *Registered to vote. Serving in Afghanistan. Never received a ballot. Tried to use the Federal Absentee Write in process - still required me to mail in the ballot and I was out of time… am very angry!*[9]

That Marine, soldier, sailor, etc. should be able to cast their ballot even if [or maybe particularly if] they didn't return to base from two months in the bush until election day itself.

Electronically returning marked ballots can eliminate or mitigate many of the present problems with overseas/military voting; the challenge is to find ways to leverage the power of electronic delivery while also protecting the integrity of the voting system.

Internet Challenges

The Internet is a digitally-dangerous place and it is critical to understand the risks and challenges before discussing specific solutions. Anonymity is fairly easy to attain on the Internet, so deterrence to committed intruders is minimized. Additionally, the opportunity

[9] https://www.overseasvotefoundation.org/files/OVF_2009_PostElectionSurvey_Report.pdf

for hacking Return-On-Investment is great and there are organizations that openly advertise on the Internet that they are available to contract for cyber-attacks. Botnets, a particularly sinister type of malicious software (or malware), are pervasive on the Internet. While we do not, and cannot, know the number of infected machines, it is not unreasonable to expect that half of all Internet-connected computers contain some malicious software.

Why is this? The Internet was engineered to foster collaboration and passing information so its architecture was not designed to handle fundamental security concerns. As is often the case, security was an afterthought.

These threats to Internet-connected computers are not just theory; they are real. Virus scanners cannot prevent virus infection and firewalls cannot keep hackers out of network-attached computers. Each of these state-of-the-art defenses can be easily overcome by sophisticated intruders.

The SERVE Project

After an early attempt to examine Internet voting in the 2000 project entitled "Voting Over the Internet" the U. S. Department of Defense commissioned a Secure Electronic Registration and Voting Experiment, or

SERVE, in 2003. Four members of SERVE's technical advisory committee that evaluated the SERVE architecture reported significant security challenges for Internet voting schemes. Among those challenges were the risk of malicious software on personally owned personal computers and the pervasive threats on the Internet against any widely implemented Internet application.

These challenges remain in place today as we still are not able to ensure integrity of arbitrary remote network nodes. The SERVE Report[10] is not alone in its skepticism regarding Internet voting. There are many sound research reports that confirm the primary risk that the SERVE Report documents.

A common question revolves around comparisons of voting to financial systems that pass literally billions of dollars a day across the Internet. The argument goes something like this: "If we can pass money around the Internet like this, why can't we vote over the Internet too?"

There are two overriding differences between financial systems and voting applications.

[10] http://www.servesecurityreport.org/

First, financial systems require records that bind a person to each transaction. Thus, there is a record of who conducted each transaction along with critical transaction details. Conversely, election integrity (and often, state law) requires that voters be irreversibly separated from their selections once their ballots are cast. This severely limits the ability to investigate irregularities, since the fundamental forensic data of who cast which ballot cannot be maintained.

The second difference between voting and financial systems is that financial systems can absorb a significant level of error and inconsistency during financial transactions, yet still maintain a positive profit margin. Voting systems enjoy no such flexibility, since even a very small error rate can result in an errant contest decision.

The fundamental problem identified in the SERVE Report turns on the proposition that we can neither prevent nor detect malicious software on privately owned computers. To date, there is no counter argument to this point. This strong theoretic result, that is consistently reaffirmed in practice, dictates that electronic marked ballot delivery systems should not employ privately owned computers, particularly not those that are connected to the Internet.

The Threat Picture

A pivotal consideration in estimating the risks of networked applications, particularly a voting application, is the size of the prospectively affected population. It is unlikely that an attacker would risk committing a felony in order to change a few votes with little likelihood of controlling a contest result. Moreover, if they do undertake a low-impact attack, the effect of success in that scenario is, by definition, low.

Conversely, as the stakes rise in terms of the size of the potential population, the cost or risk to the prospective attacker is more easy to justify.

The threat picture for voting applications for military members and their families is of low magnitude. If there are one million prospective military voters spread over more than 3,000 voting jurisdictions (and many more precincts), the opportunity for meaningful mischief is minimal.

The situation is even stronger for pilot projects with controlled, limited participation and exaggerated security procedures. The safest, most effective way to exercise and examine solutions for military voters is through government sponsored pilot projects.

The Path to a Solution

As is noted throughout the description above, the primary limitation to leveling the voting playing field for military members and their families is to reduce the ballot transmission time between voters and their local jurisdictions. The paradigm that is envisioned is a system that employs electronic blank ballot delivery and that allows the voter to attain a physical vote record that corresponds to their marked electronic ballot, with the electronic ballot being returned to their jurisdiction across an electronic network while the physical vote record is transported via courier.

While there are many technological challenges that exist, based on my thirty years of computing experience and my fifteen years experience as an information security researcher, I am convinced that it is possible to mitigate the risk of attacks on pilot projects for electronic marked ballot delivery with the following provisions:

- For a limited sized voting population
- Apply strong information security techniques
- Use a centrally owned and controlled voting station
- Capture, retain, & compare electronic and physical ballot representations for every ballot cast

Under these stipulations, government sponsored pilot projects can exercise prospective solutions that can dramatically improve accessibility and turnout for many categories of military, and overseas, voters.

Pilot projects

There have already been several pilot projects that target electronically delivering marked ballots and much progress has been made. Through these pilots, we know that military members are anxious to vote and they are excited about using computers to overcome the limitations of exclusive reliance on physical ballot delivery.

The first objective of an electronic marked ballot return pilot is to assess the functional effectiveness of the piloted approach. That is, the pilot must determine if the pilot approach works under the limited pilot environment. There must be precise, measurable success criteria and a plan to validate the results.

While functionality is the most visible pilot focus, an essential element is for the pilot to demonstrate, or at least offer evidence, that the approach used in the pilot environment can reasonably be scaled or otherwise transitioned into a reasonable operational environment; that is, the pilot must be designed to determine whether, in addition to working in the pilot

environment, the system has a good chance of succeeding under real world circumstances.

In addition to functionality, pilot projects should examine multiple architectures to optimize cost and complexity to the greatest extent possible. For example, pilots should exercise:

- Virtual private networks
- Cryptographic voting systems
- Document delivery/upload systems

Additionally, the elephant in the room in many discussions on military voting is the capability to leverage military networks in the voting process for military voter. Thus, pilots should be designed to exercise:

- Voting kiosks transmitting across military networks
- Selected military computers as voting terminals, transmitting across military networks

Pilots that exercise multiple architectures are preferable to single architecture pilots.

Finally, a pivotal aspect of any pilot must be to capture cost data sufficient to estimate implementation and maintenance costs of the exercised approach if it were to be adopted.

Summary

The very nature of their service creates tremendous challenges to providing military members and their families the capability to vote. We are a free society largely because of their sacrifices and we owe them much more than a debt of gratitude: We owe military members and their families the capability to reliably cast their ballots.

Technology exists to allow the vast majority of overseas military members and their families to access electronically transmitted elections materials. It is time to break down the barriers to leveraging that capability to its fullest in support of our military members and their families.