The Genesis and Implications of Equating "Remote Electronic Absentee Voting" with Internet Voting

Joseph Lorenzo Hall, UC Berkeley/Princeton*

23 August 2010; v1.2†

1 Introduction

The purpose of this workshop is outlined in the Call for Participation:

> "The Election Assistance Commission (EAC), Federal Voting Assistance Program (FVAP) of the Department of Defense, and National Institute of Standards and Technology (NIST) are sponsoring a workshop to explore the technical issues associated with *remote electronic absentee voting* systems for military and overseas voters."[1] (emphasis added)

While the CFP doesn't state so explicitly, it has become clear in the lead up to the workshop that the phrase "remote electronic absentee voting" (REAV) is intended to refer to voting over the internet from personal computers.

It's not clear from the legislative record from where this interpretation arose. In this short paper, I aim to describe, to first order, what the law and legislative record say and connect this back to possible implications for narrowly defining the future of UOCAVA voting solutions.

2 Legislative Intent

In this section I will examine what the law actually says and what the various Congressional Committee Reports and Conference Committee Reports tell us about the intent behind establishing an electronic absentee voting pilot project program.

2.1 What the Law Says

The posture that "remote electronic absentee voting" is equivalent to internet voting is perhaps most evident in the EAC's status report to congress in compliance with the MOVE Act,[2] where EAC describes their current efforts as developing "guidelines for remote electronic absentee (i.e.,

*This paper was authored for the EAC/FVAP/NIST *Workshop on UOCAVA Remote Voting Systems* to be held 6–7 August, 2010 in Washington DC. Author's website: http://josephhall.org/; Contact: joehall@berkeley.edu.

†This is a later version of this paper than the version originally submitted to the workshop (v1.0; 30 July 2010), benefiting from additional work and/or information from others. If you'd like a copy of a previous version, just ask.

[1] *See:* http://www.nist.gov/itl/csd/ct/uocava_workshop_aug2010.cfm.

[2] MOVE required EAC to issue a report to Congress if it hadn't "established electronic absentee voting guidelines" by 180 days after MOVE was enacted. *See:* Public Law 111-84. *Military and Overseas Voter Empowerment Act (MOVE Act)*. 2009. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_public_laws&docid=f:publ084.111, §589(e)(2).

Internet-based) voting systems to support the voting needs of military and overseas citizens."[3] In that document, EAC goes on to say,

> "In addition, MOVE reiterated the 2004 mandate from Congress requiring EAC to create guidelines to be used by FVAP for the development of a remote electronic voting system."[4]

MOVE was enacted as § 575 *et seq.* of the National Defense Authorization Act (NDAA) for Fiscal Year 2010. Section 589(e)(1) of that Act requires NIST and EAC to provide FVAP with:

> "best practices or standards in accordance with electronic absentee voting guidelines established under the first sentence of section 1604(a)(2) of the National Defense Authorization Act for Fiscal Year 2002 (Public Law 107-107; 115 Stat. 1277; 42 U.S.C. 1977ff), as amended by section 567 of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108-375; 118 Stat. 1919) to support the pilot program or programs."[5]

To adequately parse this last section, the language of these previous two defense appropriation acts from 2002 and 2005 provide context. The "first sentence of section 1604(a)(2) of the National Defense Authorization Act for Fiscal Year 2002" says:

> "AUTHORITY TO DELAY IMPLEMENTATION.—If the Secretary of Defense determines that the implementation of the demonstration project under paragraph (1) with respect to the regularly scheduled general election for Federal office for November 2002 may adversely affect the national security of the United States, the Secretary may delay the implementation of such demonstration project until the regularly scheduled general election for Federal office for November 2004."[6]

and "section 567 of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005" amended this with the following language:

> "The first sentence of section 1604(a)(2) of the National Defense Authorization Act for Fiscal Year 2002 (Public Law 107-107; 115 Stat. 1277; 42 U.S.C. 1977ff note) is amended by striking 'until the regularly scheduled general election for Federal office for November 2004' and inserting the following: 'until the first regularly scheduled general election for Federal office which occurs after the Election Assistance Commission notifies the Secretary that the Commission has established electronic absentee voting guidelines and certifies that it will assist the Secretary in carrying out the project'."[7]

---

[3] U.S. Election Assistance Commission. *Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems*. Apr. 2010. URL: `http://www.eac.gov/assets/1/AssetManager/2010-04-26%20Report%20Congress%20EAC%20Efforts%20Establish%20Remote%20Electronic%20Absentee%20Voting%20Systems.pdf`, at 1.

[4] U.S. Election Assistance Commission, see n. 3, at 1.

[5] Public Law 111-84, see n. 2, §589(e)(1).

[6] Public Law 107-107. *National Defense Authorization Act for Fiscal Year 2002*. 2001. URL: `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ107.107.pdf`, §1604(a)(2).

[7] Public Law 108-375. *Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005*. 2004. URL: `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ375.108.pdf`, §567.

The legislative mandate seems clear: EAC and NIST must create "best practices or standards" for electronic absentee voting and EAC must certify its willingness to assist FVAP before the Department of Defense can engage in any pilot projects under this legislation. What is not clear is what the term "electronic absentee voting" means, nor what the difference is between that term and the construction used by FVAP, EAC and NIST (which adds "remote" to the beginning of the phrase).

2.2 What the Committee Reports Say

For insight, a useful place to find indications of legislative intent is in the Congressional Committee Reports issued by the various committees in Congress that considered a given piece of legislation. The next section will focus on the Conference Reports—produced in the process of reconciling differing legislation passed by both houses of Congress—that might show collective legislative intent across the Congress. These Committee Reports will more specifically speak to concerns and intent from individual committees.

In their report on the 2002 NDAA, the Senate Committee on Armed Services said the following, referring to the perceived success of a previous internet voting pilot project from 2000:

> "In the committee's view, the Federal Voting Assistance Program's Voting Over the Internet (VOI) Pilot Project is an important first step in assessing how to use the internet to enhance absentee voting. This pilot demonstrated that a remote internet registration and voting system can provide electoral process integrity; it reduced traditional barriers to participation in elections by absentee voters; and it provided insight into issues that must be considered for broader use of remote registration and voting via the internet. *The committee encourages the Department of Defense to build on the experience gained in this groundbreaking project with a follow-on demonstration project designed to ensure a judicious and methodical progression from the current by-mail process to a secure, easy-to-use, and expedient remote internet registration and voting system.*"[8] (emphasis added.)

This, as will become apparent, is the most clear statement of intent in terms of advocating for internet-based methods of absentee voting.

The associated report for the 2002 NDAA from the House's Committee on Armed Services is not as clearly enthusiastic about specifically internet voting:

> "The committee, which was deeply disappointed that military absentee voters were not offered consistently high quality voting information and assistance during the 2000 election, recommends a series of voting initiatives designed to improve the ability of the Department of Defense managers to comply with the requirements of the Federal Voting Assistance Program and related law. [...] Included among the initiatives is the testing of electronic voting systems that aim to solve the time and distance challenges that have plagued military voters, particularly those residing at overseas duty locations.[9] [...]
>
> "Section 552–Electronic Voting Demonstration Project: This section would require the Secretary of Defense to carry out a demonstration project to allow military absentee voters to vote using an electronic voting system. This section would require the Secretary

[8] Committee Report 107-62. *National Defense Authorization Act for Fiscal Year 2002*. 2001. URL: `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_reports&docid=f:sr062.107.pdf`, at 307.

[9] Committee Report 107-194. *National Defense Authorization Act for Fiscal Year 2002*. 2001. URL: `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_reports&docid=f:hr194.107.pdf`, at 307.

to coordinate with state officials to facilitate the demonstration project. The committee expects the Secretary to actively encourage state election officials to participate in the demonstration project and to take all prudent steps to expand the demonstration project to reach as many military voters as possible. *The committee believes that the method for absentee voting that holds the most promise for protecting the voting rights of military members in the future is electronic voting using computers.*"[10] (emphasis added.)

A similar set of statements occurs in the committee reports surrounding the 2005 NDAA. The Senate Committee on Armed Services Report expresses disappointment in the canceling of the 2004 demonstration project (SERVE), and encourages subsequent pilot projects, that can be postponed for cause, in 2006 and 2008:

> "Section 1604 required the Secretary of Defense to carry out a demonstration project in which absentee uniformed voters would be permitted to cast ballots using an electronic voting system in the general election for federal offices in November 2002. Pursuant to the Secretary's authority to delay implementation, the demonstration project was postponed until November 2004 to plan for an Internet voting option called Secure Electronic Registration and Voting Experiment (SERVE), involving 51 counties in seven States and as many as 100,000 military personnel, was well underway. In February 2004, the Department concluded that the SERVE program could not sufficiently ensure the legitimacy of votes cast in the November 2004 election, and sought authority to further delay the electronic voting demonstration project.
>
> The committee recognizes the effort by the Department of Defense, working in concert with state, county and federal election officials, to bring the SERVE program to fruition, and urges continued examination of feasible means to carry out secure electronic voting. If the Department determines, however, that the implementation of such a demonstration project in 2006 may adversely affect the national security of the United States, the Secretary may further delay implementation until 2008."[11]

This appears to be an important shift from this Senate Committee: it recognizes that the SERVE program, an internet voting project, was unable to "sufficiently ensure the legitimacy" of those votes and the Committee encourages future examination of "secure electronic voting".

The associated report from the House Committee on Armed Services for the 2005 NDAA simply expresses disappointment that the integrity of the election process might have been put at risk, but remains silent about encouraging future pilot demonstration projects:

> "Section 592–Repeal of Requirement to Conduct Electronic Voting Demonstration Project for the Federal Election to be Held in November 2004: This section would repeal the requirement in section 1604 of the National Defense Authorization Act for Fiscal Year 2002 (Public Law 107-107) for the Secretary of Defense to conduct a demonstration project to permit absentee uniformed service voters to cast their ballots through an electronic voting system. The committee regrets that the Deputy Secretary of Defense believed he had no option but to terminate the electronic voting demonstration project, but the committee understands that the decision was necessary to avoid any risk that the demonstration project would threaten the integrity of the election process."[12]

[10] Committee Report 107-194, see n. 9, at 320.

[11] Committee Report 108-260. *Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005*. 2004. URL: `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_reports&docid=f:sr260.108.pdf`, at 381.

[12] Committee Report 108-491. *Ronald W. Reagan National Defense Authorization Act for Fiscal Year*

Finally, The various committee reports for the 2010 NDAA contain no statements relevant to the demonstration pilot program.

2.3 What the Conference Committee Reports Say

The next possible place to look for legislative intent as to these terms is in the Conference Committee Reports for the various laws above. Recall that when both houses of Congress pass legislation, the differences between the versions as passed must be worked out in a conference committee before the final legislation can be delivered to the President's desk. These conference committees produce a report that may have indicia as to the legislative intent behind the final form of the law.

For the 2002 defense appropriations act, the conference committee report contained only substantive comments about DOD concerns of rushing a demonstration in 2002 and a request that DOD look to commercial off-the-shelf technologies to allay their concerns:

> "The conferees are aware of the Department's concern about having sufficient lead time to prepare for a meaningful demonstration project in 2002. The conferees encourage the Department to consider use of commercially available, off-the-shelf, electronic voting products to expedite preparation for the 2002 demonstration."[13]

For the 2005 act, the conference committee report states a much more interesting, for our purposes, comment:

> "The conferees recognize the magnitude of the technical challenge associated with ensuring the security of electronic voting using the Internet. The Department of Defense's Secure Electronic Registration and Voting Experiment (SERVE) was an important prototype for electronic voting that should not be abandoned. The conferees encourage the Secretary to provide funding to the Election Assistance Commission and the National Institute of Standards and Technology to advance electronic absentee voting by U.S. voters located overseas and Uniformed Services voters."[14]

This clearly encourages future experimentation with electronic voting, but any mention of the internet is conspicuously missing.

Finally, the conference committee report for the 2010 defense authorization was entirely silent as to any substantive comment on the part of the MOVE act that explicitly requires EAC and NIST to develop REAV/EAV best practices or standards.[15]

2.4 Discussion

I have not had adequate time to examine Congressional floor statements surrounding these laws, so I am unsure if those materials or, perhaps, other sources of legislative intent might better clear up the scope of the term.[16]

2005. 2004. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_reports&docid=f:hr767.108.pdf, at 327.

[13] Conference Report 107-333. *National Defense Authorization Act for Fiscal Year 2002*. 2001. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_reports&docid=f:hr333.107.pdf, at 734.

[14] Conference Report 108-767. *Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005*. 2004. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_reports&docid=f:hr767.108.pdf, at 680.

[15] Conference Report 111-288. *National Defense Authorization Act For Fiscal Year 2010*. 2009. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_reports&docid=f:hr288.111.pdf, at 747.

[16] Certainly, if a reader knows of other indicia of legislative intent that I have obviously missed, please let me know.

With that caveat, the text of these laws and the conference reports paint a vague picture. No where is it clear that either the REAV or EAV terms should be narrowed in scope sufficiently to mean casting ballots over the internet from voters' personal computers, without a source of end-to-end auditability, be that cryptographic or a physical audit trail. What is clear is that internet voting pilot projects were decidedly in scope in the 2002 legislation and then the intent of Congress seems to emphasize "secure electronic voting" rather than necessarily internet-based forms of REAV/EAV. The silence from the Congressional record around the most recent round of amendment to this legislation (via MOVE) does nothing to emphasize that internet-enabled models, or any specific model, should be specifically considered for pilot projects.

3 Implications of a Narrow Definition for REAV/EAV

The consequences of adopting a narrow view of the REAV or EAV terms are profound.

The broadest notion of remote voting includes all forms of voting that don't take place in a traditional polling place. Figure 1 is a stylized illustration of various current, future and some very fanciful possibilities for remote voting architectures. Voting over the internet from PCs is only one class of these kinds of systems, and there are at least three distinctions that are important and deserve adequate attention.

3.1 Controlled and Supervised Architectures

The remote voting methods along the bottom of Figure 1 are *controlled* architectures operating in *supervised* environments. In systems with controlled architectures, the election official has responsibility for ensuring the trustworthiness of voting system hardware, software and chain of custody. One of the most serious issues with the current conception of REAV as "internet voting" is the susceptibility of user-controlled platforms to malware and general disrepair. When the election official has this responsibility, risks due to malware or disrepair must drop significantly (granted,

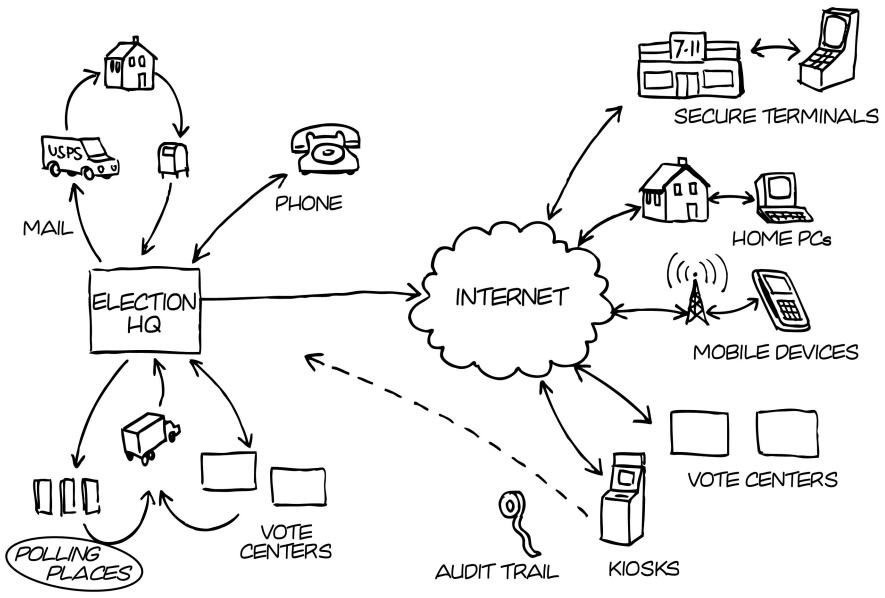

Figure 1: Polling-place voting (lower-left) is increasingly being augmented by forms of *remote voting*.

assuming that the platform isn't fundamentally subvertable to start with, which is not a very robust assumption).

In supervised environments, an agent of the election official, typically a poll worker, is trained to run the election and ensure specific procedural parameters are not violated. In addition to providing interactive personal assistance to voters who may encounter barriers to casting their ballots, poll workers also serve as the front line in terms of spotting suspicious activity and ensuring that voters are voting free from coercive or material influences.

Of course, traditional vote-by-mail is also an unsupervised environment, but with considerably more control over cast ballot transmission and, importantly, the voter can choose to return their ballot in a variety of ways, not just through the postal service. The forms of voting considered under the current conception of REAV need to afford these kinds of choices and limit the use of these systems to only those voters who can demonstrate hardship.

3.2 Kiosk-based Architectures

A fledgling form of remote voting involves using controlled kiosks in supervised environments; this architecture was piloted during the Okaloosa Distance Balloting Project.[17] Many of the same issues that will arise with large-scale REAV models will also be relevant to scaled kiosk models in terms of logistics and information assurance but without the significant changes entailed by using public networks, users' PCs and voting systems with no end-to-end auditability. Despite the enthusiasm and momentum for internet voting, it would seem prudent to focus on incremental architectures like kiosk models where various elements of the system could be relaxed incrementally, as the technology and needed procedures mature.

3.3 Implications for Auditability

Finally, the rise of internet voting appears very similar to the rise of voting on DREs in the wake of the 2000 presidential fiasco. Auditability of both these types of systems is a real concern.

To be clear, auditors generally perform two types of audit activities: *process audits* and *materiality audits*. Process audits are designed to make sure procedures have been followed to the best of the system's ability. In the voting context, examples of process audits include ballot reconciliation—where the auditor reconciles the original number of blank ballots against all the types of ballots received from a polling place against the records of spoilage, voter signatures, etc.—and chain of custody checking—where an auditor checks to see that an unbroken chain of documented custody exists for various critical pieces of equipment.

Materiality audits focus on the accuracy of the bottom-line numbers such that all independent records that can be used to arrive at estimates of the results are examined to a certain level of confidence for material discrepancy. In voting, this is fundamentally about post-election audits, be they manual tally audits or machine-assisted audits.[18]

[17] *Procedures and System Description for Secure Remote Electronic Transmission of Ballots for Overseas Civilian and Military Voters.* Operation BRAVO Foundation. June 2008. URL: `http://election.dos.state.fl.us/voting-systems/pdf/ODBPplanJune_19.pdf`.

[18] Joseph Lorenzo Hall, Luke W. Miratrix, Philip B. Stark, et al. "Implementing Risk-Limiting Post-Election Audits in California". *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections 2009 (EVT/WOTE 2009)* (Aug. 2009). URL: `http://www.usenix.org/events/evtwote09/tech/full_papers/hall.pdf`; Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. "Machine-Assisted Election Auditing". *USENIX/ACCURATE Electronic Voting Technology Workshop 2007* (Aug. 2007). URL: `http://www.usenix.org/events/evt07/tech/full_papers/calandrino/calandrino.pdf`.

Any system that does not support both kinds of auditing is not fully auditable. Systems that are designed to support only process audits or materiality audits or where auditors don't have the access needed to perform specific types of audits cannot be said to be auditable. Because these classes of systems cannot be fully audited, it will be difficult to prove to a certain level of confidence that the winner the election declares was indeed the true winner. More importantly, the performance requirement of software independence cannot be met by a system that does not support these kinds of audits (other than, curiously, lever machines which cannot support materiality audits but do not have software).

4 Conclusion

The REAV term is unfortunately vague, and narrowing it to "internet voting" has significant implications for security, privacy, and auditability.

As I outline above, there is relatively little support, from the text of the law and indicia of legislative intent in the form of committee and conference reports, for the premise that "electronic absentee voting" was meant to be construed as uncontrolled, unsupervised forms of voting over the internet without end-to-end auditability. The implications of using such a narrowly-constructed term means than no supervised and/or controlled architectures are going to be considered for these pilots.

The present terminology adoption surrounding the upcoming NIST UOCAVA Workshop that considers electronic voted ballot return architectures exclusive from personal computing devices unnecessarily limits the options available to military and overseas voters in response to the MOVE Act to the pilots that will be conducted there under.

In conclusion we recommend rethinking the terminology that limits states in conducting electronic absentee balloting to personal PCs and urge you to consider architectures that involve secure point-to-point security and in their application and communications architecture.