POSITION PAPER SUBMITTED TO NIST – FVAP – EAC UOCAVA SUMMIT

Essential Baseline Research for UOCAVA-MOVE Act Implementation at the State - Local Levels

Matt Bishop (University of California, Davis) & Candice Hoke (Cleveland State University)
bishop@cs.ucdavis.edu shoke@me.com

Abstract

Three major Federal legislative enactments seek to enable overseas and military voters to cast valid ballots securely in Federal elections. The most recent legislation includes federal mandates and preemptive provisions that require State and local election administration officials to offer their overseas voters the ability to transmit materials electronically, such as remote voter registration forms and absentee ballot applications. This paper contends that our current knowledge of the technical and security infrastructure that exists at the State and local election administrative offices is insufficient to enable the UOCAVA and MOVE Acts to be fully realized while concomitantly protecting the integrity of Federal elections. Topical areas for independent research by qualified experts include voter information privacy protections and defense-in-depth security policies and practices – the latter of which relates closely to achieving system and service reliability and data integrity and accuracy. The paper contends that if electronic "best practices," technical and security standards, and other Federal election policies are promulgated without sound baseline knowledge of existing conditions, serious but avoidable problems are likely to arise. These include (1) ***Phase–In Planning Omissions*** *arising from potentially false assumptions regarding the technical infrastructural status quo; (2)* ***Insufficient Budgets*** *for ongoing technical and security management that may undermine election success and MOVE Act implementation; and (3)* ***Voter Privacy, Security, and Reliability Objectives*** *that may be undermined with significant new yet avoidable risks that may not be manageable within the current infrastructure, and thus not effectively remedied. Thus, policymakers and standards-setting agencies cannot meet the larger public interest and MOVE Act objectives without sound data (which can be anonymized to exclude names of the jurisdictions) and expert evaluations of the existing technical infrastructure within which local and State election administrators must function.*

I. Introduction

During the last half-century, the nation's global military roles combined with expanding global commerce have resulted in millions of United States citizens living abroad. American expats reside in European, Asian, Middle Eastern, and Latin American locations, often with their families living abroad with them. These overseas military and civilian Americans have often faced insurmountable hurdles to their casting valid absentee ballots (AB) from remote locations, especially because they come from all over the country—and the fifty states and District of Columbia, differ, often dramatically, in their prerequisites for absentee voting.

Congress has recognized the effective disenfranchisement of vast numbers of American citizens abroad and the particular injustice of voting barriers to uniformed service members. In response, it has tried to eliminate these impediments and augment overseas voters' abilities to cast valid ballots that will be counted. The most recent and broad-based remedial federal legislative efforts began in 1986 with the *Uniformed and Overseas Citizens Absentee Voting Act* ("UOCAVA"). The *Help America Vote Act* ("HAVA" 2002) and the *Military and Overseas*

Voters Empowerment Act ("MOVE" 2009) have expanded and modified these earlier mandates to assist overseas citizens, who are often called "UOCAVA voters."

Embedded within these three Acts are two distinct policy trends. First, they increase the federalization of absentee ballot procedures, thereby pre-empting conflicting State election laws. Second, the new Federal mandates intensify deployment of computer and network technologies, including requirements for unspecified electronic voting pilot projects.

Significantly, the effects of these trends and mandates are affecting not only UOCAVA voters, but also voters residing in the United States by causing rapid changes in State and local election practices. Once new technologies and managerial systems have been introduced for a particular segment of voters, internal and sometimes fiscal pressures arise to unify systems. Thus technological changes for one segment of the electorate are often generalized to the whole.

These federal legislative efforts are motivated by the laudable objective of realizing fully the voting rights of overseas civilian and uniformed service members. Yet, the new mandates require deployment of electronic technologies in mission-critical areas of election administration, thereby introducing exposure to significant new risks. These risks may not be fully understood by election officials and policy makers who lack significant network and computer security expertise. Even when local election and state officials recognize some of the new risks, particularly those posed by Internet connectivity, they may lack the technical and security infrastructural support essential for assuring election success and electoral integrity. For example, the NIST-EAC Information System Security Best Practices for UOCAVA-Supporting Systems (Draft NISTIR 7682) will not be applied effectively if qualified technical personnel are not available to implement and monitor the practices, or if essential equipment is not supplied, or other necessary components omitted. This "information gap" has generally been overlooked.

This paper outlines the research needed to facilitate implementation of the MOVE Act without exposing the States' election systems and the people's voting rights to perilous new risks. It identifies several serious yet unintended consequences if the information gap is not remedied promptly. Finally, it proposes next steps to conduct the research and supply the evaluations that will permit the MOVE Act's promise to overseas voters to be fulfilled in a context of greater assurance of electoral administrative proficiency and accuracy.

II. New Mandates and Options for Electronic Fulfillment of Voting Qualification Tasks

One of the most significant impediments to UOCAVA voters casting valid ballots lies in the transmission time needed to complete each required sequential step in the voting process. A person must register to vote, apply for and receive a blank absentee ballot, and return the marked ballot within the permitted period. The MOVE Act modifies time limits for some tasks. However, MOVE's more favored tactic is to require States to offer UOCAVA voters the option of using an electronic transmission for completing most, but not all, election tasks.

Notably, the Act does not mandate the ***substitution*** of electronic for traditional postal mail. Instead, it generally requires States to supplement their traditional administrative processes with at least one electronic mechanism, and to ***offer*** their overseas voters the ***choice*** of using this mechanism for any or all of the authorized transmissions.

The electronic information transmissions that the MOVE Act requires States to offer includes voter registration applications, absentee ballot applications, voting information and notifications (including federal candidates) for using the Federal write-in ballot, and blank ballot transmission.

Although the MOVE Act does not mention electronic transmission of voted ballots as a mandated option (and arguably impliedly forecloses that option), at least 20% of all States

now offer some option of electronic transmission of marked ballots. A significant number of these States permit voted (marked) ballots to be returned as email attachments.

III. Factors Affecting Implementation of Sufficient Security and Privacy Protections

Some observers might suggest that States and localities already have a significant interest in successful election administration of both Federal and State elections, and that such success naturally entails adequate technical security and voter privacy protection. Thus, Federal Government standards-setting entities need not seek an empirical baseline regarding the technical and security infrastructures currently in place. They might recommend that NIST, EAC and FVAP simply conclude that State governments have attained sufficient protection of technical election security.

Such an argument might have carried more persuasion previously and may again in several years. However, several factors can be identified that militate against States' maintaining the security infrastructures needed for MOVE Act and pilot project implementation. These include: (a) significant State and local budgetary shortfalls, deficits and reductions in personnel throughout most of the nation; (b) a diversity of local administrative structures, personnel, and funding apparatus for elections, some of which may be less well funded and equipped than others; (c) smaller jurisdictions' increased use of outsourced technical support, without internal technical quality control and assurance; (d) lack of cyber security understandings and practices within the population as a whole, as documented in other federal reports;[1] (e) the omission of technical security expertise within much of the local election official (LEO) community (and sometimes as well in the Secretary of State staff); (f) the rapid timetables for implementation of MOVE and HAVA, possibly leading to incomplete security infrastructure; and (g) numerous federal agencies and departments continuing to fail to meet information security standards, as documented by the GAO.

IV. Empirical Baseline Relevance to the MOVE Act "Practicability" Directive

The MOVE Act arguably recognizes that election security and voter privacy interests might be threatened by its electronic technology initiatives. Thus, the Act singles out these two technical and functional attributes for particular attention and imposition of duties. (*See, e.g.*, MOVE Act, § 577(a)(2) *codified at* 42 USC §§ 1973ff-1(e)(6) Security and Privacy Protections, largely repeated at § 578).

The Act's language on these points is noteworthy, for it does not impose an abstract duty but rather a standard that can be realized. For instance, "***To the extent practicable***, States shall ensure [their] procedures. . . protect the security and integrity of absentee ballots." § 577(a)(2). Similar phrasing describes the States' duties to protect voter privacy interests.

Legislative use of the modifier "practicable" generally imports feasibility considerations when construing the language to determine standards of conduct or protection imposed. Here, the term contemplates a realistic, achievable, reasonability approach to determining procedural practices and standards for ballot integrity and security. One might argue Congress recognized that no electronic information technology is foolproof, and so imposed an achievable level of security.

Nevertheless, one major question that arises is whether the legally required feasible, realistic level of security protection and voter

[1] For instance, President Obama's Cyberspace Policy Review includes among the ten immediate priorities: "6. Initiate a national awareness and education campaign to promote cybersecurity." http://www.whitehouse.gov/administration/eop/nsc/cybersecurity. See also E. Fischer, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options* 23-24 (Congressional Research Service 2005).

privacy will be achieved in the absence of an empirical and evaluative baseline. Where federal security metrics and protocols are promulgated without cognizance of current infrastructural conditions for technical election management, the resulting standards could easily be unrealistic for State implementation.

As such, the security standards arguably might fail a legal challenge of achieving the congressional directive of being "practicable." Worse, however, the standards or best practices documents may be sufficiently far from current practices and infrastructural realities that the State and local election administration ignore the recommendations or are overwhelmed with the range of tasks given the gap between the standards and their technical-security infrastructural context. Some documents may also be incomprehensible or only thinly understood if the requisite computer security personnel and expertise are not part of their election administrative apparatus charged with implementation.

In addition to supporting the constructing of standards that are practicable and useful, an empirical and evaluative security and privacy baseline would facilitate at least three additional election administrative objectives. First, this research can provide documentation that is needed to support **budgetary appropriations** to sustain (or create) the infrastructure for achieving security and privacy objectives. Second, having the baseline evaluations would promote consideration of issuing security standards (including metrics and protocols) in a multi-year, **phased implementation approach**, rather than as a solitary set of arduous standards that are possibly unrealistic for the current election administrative conditions. Third, the research could provide opportunities for **early identification and remedy** of new risks to privacy, security, and reliability objectives that may have been generated by rapid attempts to comply with the MOVE Act electronic requirements. Overall, the research could promote the crafting of better standards more likely to be implemented, and thereby provide greater protection of security and voter privacy concerns as well as election success.

V. Moving Forward the Essential Research Agenda

A. **Structuring and Funding the Research Project**: Both NIST and the EAC have received federal research appropriations to support independent research for elections administrative improvement. NIST has expertise in computer and network security research, and the role of supplying technical advice and proposed standards to the EAC. Thus, it should solicit research proposals for conducting the baseline research identified here, select the team or teams to conduct this research, and receive the research reports.

B. **State and Local Election Officials' Voluntary Participation and Anonymizing of Data**: In many States, election administration is a politicized arena. To promote research participation and obviate political censure, the research project would need to use anonymized data from elections and elections offices, both State and local. Whether researchers also provide particularized reports and recommendations to the State or local election offices that are participating in the research project should be a choice left to the participating organizations.

C. **Scope of the Research**: As part of the scope of work, NIST should construct collaboratively with the research team(s) a conceptual and statistical framework for capturing data; the rubrics or metrics for assessment of defense-in-depth[2] practices and policies for all technical

[2] Defense in depth or layered security has become a basic principle of computer security design and management. *"The principle of separation of privilege states that a system should not grant permission based on a single condition."* M. Bishop, Computer Security: Art and Science (2002). Thus, if one defense fails, is penetrated or is bypassed, other defenses will remain effective. *See also* Jerry H. Saltzer & Mike D. Schroeder *The Protection of Information in Computer Systems*, *Proceedings of the IEEE* 63 (9): 1278–1308 (1975)

systems that support federal elections; and methods for researchers' observing and collecting data during election cycles, including Election Day. Analysis should include attention to information and managerial gaps, development of prioritized recommendations for technical and managerial mitigations; protocols and best practices for layered security and ongoing technical oversight in light of the security infrastructural baseline; and discussion of educational programming for election officials that can empower them to augment technical security in their offices.

Conclusion

Implementation of the MOVE Act, including its requirements to achieve sound security and protect voter privacy, depends on obtaining a clear picture of the technical and security infrastructural status quo. This paper argues that unless tethered to current reality, "best practices" guidance, recommendations for achieving layered security, and standards setting may be pervaded with avoidable flaws. These policies may thereby also risk non-implementation by election administrators. Independent research to document the diversity of technical and security infrastructures throughout the nation would enhance full performance of the roles Congress assigned NIST, FVAP and EAC and effective implementation of federal MOVE Act objectives.

———————

Note:
Both authors have had the pleasure of working closely with local and State election administrators on achieving technical security. They welcome deeper discussion of the proposed project outlined here and its value to election administrative objectives and voting rights.

---

http://web.mit.edu/Saltzer/www/publications/protection/.

Background on Authors:

Matt Bishop is a professor in the Department of Computer Science at the University of California at Davis, where he is a co-director of the Computer Security Laboratory. His research specializes in the analysis of computer system vulnerabilities, the design of secure systems and software, network security, formal models of access control and user authentication. He has authored the textbooks *Computer Security: Art and Science* and *Introduction to Computer Security*. He has participated in several scientific analyses of electronic voting systems, including the forensics analysis of the problematic 2006 contested Florida congressional district CD-13 race and the RABA 2004 review of Maryland's e-voting systems. He was a co-Principal Investigator for the California Top-to-Bottom Review (2007). Prof. Bishop has been a member of the Voting Systems Technology Assessment Advisory Board for the State of California. He worked closely with California policymakers in drafting legislation to augment information security in public IT systems that the Legislature enacted. He continues to work with his county Clerk-Recorder on election security and with other local and State election officials.

Candice Hoke is the founding Director of the *Center for Election Integrity* and a law professor at Cleveland State University with Election Law and Regulatory Law expertise. Her primary research focuses on regulatory and operational issues raised by new election technologies such as on-line voting. She is a member of the American Bar Association's Advisory Commission to the Standing Committee on Election Law (2007-present). She was a research Team Leader for the California Secretary of State's scientific study of voting systems (TTBR, 2007), and a member of the Cuyahoga Election Review Panel (2006) that examined the causes and cures for major election failure. She served as Project Director of the *Public Monitor of Cuyahoga Election Reform* (2006-08), authoring reports on election technical security. She proposed and led the first post-election audit in Ohio (November 2006). She has drafted proposed federal election cybersecurity legislation and Ohio election reform legislation, and has testified before Congress and the EAC on assuring public trust in election technologies. Before becoming a law professor, she was a *Yale Law Journal* editor, a judicial clerk for the U.S. Court of Appeals for the First Circuit, and a staff member of the North Carolina Governor's Office.