From: Jeremy Epstein
To: votingsystemguidelines
Subject: Comments on UOCAVA Pilot Program requirements
Date: 04/29/2010 11:24 AM

Dear Commissioners,

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

Almost everyone likes chocolate cake, but that doesn't mean it's nutritious. So it is with Internet voting - we know that it's popular as a concept, but that doesn't mean it's a good idea, any more than drunk driving might be - it's a thrill, but it's dangerous to both the driver/voter and society.

Regarding the specifics of the proposed pilot program guidelines, my biggest concern in reading the document is about an accurate threat model. The threats to an Internet voting pilot are not the same as the threats to an Internet voting system that is used in a real election, but the threat model needs to anticipate the threats against a fully operational system. The Internet is a dangerous neighborhood, and getting worse by the day. As the recently disclosed successful Aurora attacks against Google (and dozens if not hundreds of other companies) have shown, even the most sophisticated companies and government agencies with very large security budgets are routinely penetrated by determined attackers - and those attacks aren't discovered for months or years after they occur. There is no reason to believe that the small companies that are likely to run Internet voting trials, or the state and local governments that hire them, are any more likely to have the skills or technology to keep out determined adversaries. And there's little doubt that determined adversaries, whether domestic or foreign, will make efforts to influence our elections. Thus, it is critical that the threat model for any pilot programs be at the "nation state" (or highly determined, well skilled, and well funded) adversary level, and not simply "script kiddies" making a relatively uninformed brute force effort to attack the systems. Otherwise, we'll discover that the pilot programs have no problems, only to discover that the system is quickly compromised when it enters production usage where the results can change election outcomes.

Said another way, taking a car for a test drive (or even bumping it slowly into a wall) tells very little about how well it will survive in a head-on collision. But if you intend to survive a crash, you need to understand the properties of the car in that circumstance.

My second (and highly related) concern is that the security testing for UOCAVA pilots be done by companies or individuals who are not part of the VSTL lab system. The labs have skill sets in understanding the voting system requirements, but they are not experts in emulating the behavior of an adversary breaking into a system. Use of penetration testing experts will ensure that the Commission and the public will know that the testing has been performed by an organization that does not have a conflict of interest with the equipment certification.

I applaud the Commission for its interest in public comments, and am available if any clarification of my comments is needed.

Sincerely,

Jeremy Epstein

[redacted]