A Consideration of Voting Accessibility for Injured OIF/OEF Service Members: Needs Assessment

July 2012

Contract E4064914
2010 Voting Technology and Accessibility Research – Military Heroes Initiative
CFDA #90.403

PREPARED FOR:
Election Assistance Commission
1201 New York Avenue, N.W.
Suite 300
Washington, D.C. 20005

PREPARED BY:
Human Systems Integration Division
Electronic Systems Laboratory
Georgia Tech Research Institute
Georgia Institute of Technology
Atlanta, Georgia 30332

Annotated Literature Review Results

Security & Privacy Issues in Voting

Dawkins, S. & Gilbert, J. E. (2010). *An approach for anonymous spelling for voter write-ins using speech interaction.* Paper presented at the NAACL HLT 2010 Workshop on Speech and Language Processing for Assistive Technologies, Los Angeles, CA.

> Users should be able to vote and verify their ballots in private, without assistance. It is difficult to ensure voter privacy with a voting machine that uses speech input. It is particularly difficult to enabled private write-in voting by users with upper mobility impairments. The authors describe a novel system (Prime III) to provide a solution. The system uses speech input and name prediction to allow voters to verbally yet privately spell a Reagan candidate. Voters select from numbered clusters of letters by speaking the respective numbers. Then they select a numbered letter from within that cluster. An empirical study found that the novel system was both effective and efficient.

Haas, B. (2006). *Engineering better voting systems.* Paper presented at the DocEng'06 ACM symposium on Document Engineering, Amsterdam, Netherlands.

> This paper outlines some of the requirements of a voting system to guarantee trustworthy elections. These requirements include privacy, free will, reliability, prevention against ballot fraud, prevention against ballot trade, accessibility, affordability, and simplicity and usability. Because strong security often conflicts with usability, the potential for large-scale mistakes should be of greater concern than small-scale mistakes in the tradeoff between usability and security. The author also compares remote voting to poll voting and electronic ballots to paper ballots. While poll voting is more costly and complex than remote voting, it is nearly impossible to ensure the security and secrecy of ballots in remove voting. Voters generally prefer electronic ballots over paper ballots, but the potential for systematic mistakes and security breaches is greater. Given these considerations, the worst possible voting system in terms of security is internet voting and the best possible voting system includes a paper trail. Specifically, the author recommends a combination of electronic voting with a paper trail and voting by mail.

Keller, A. M., Mertz, D., Hall, J. L., & Urken, A. (2004). *Privacy issues in an electronic voting machine.* Paper presented at the 2004 ACM Workshop on Privacy in the Electronic Society, Washington, DC.

> The Open Voting Consortium's electronic voting system provides voter privacy and review capability. Unlike many other Direct Recording Electronic voting machines, the Open Voting Consortium's machine uses open source software that can be inspected by the general public. The machine also improves voter privacy by implementing bar codes on printed ballots; transparency of poll worker software used to activate smart cards (which in turn are used by voters to activate voting machines); and providing private, audible readouts to blind voters.