May 25, 2005

Ms. Juliet Thompson
General Counsel
United States Election Assistance Commission
1225 New York Avenue, N.W.
Suite 1100
Washington, DC 20005
Delivered via fax and e-mail: 202-566-1392, guidance@eac.gov

Dear Ms. Thompson,

As members of a commissioned study by the Association for Computing Machinery (known as the ACM Committee on Guidelines for Implementation of Voter Registration Databases, hereafter referred to as "the committee"), we write to comment on the Election Assistance Commission's (EAC) Proposed Voluntary Guidance on Implementation of Statewide Voter Registration Lists. We recently submitted testimony to the Commission during its April 26 public hearing on this draft guidance. That testimony[1] outlines our study's technical focus and some of the likely topics we will cover, including reliability, accuracy, and privacy.

STATES NEED MORE DETAILED TECHNICAL GUIDANCE ON A BROADER SET OF ISSUES

The committee applauds the Commission's work toward providing states with guidance on implementing the voter registration databases mandated by the Help America Vote Act (HAVA). States will face many technical challenges in implementing these databases in a secure, accurate, and reliable manner, while protecting sensitive information and minimizing the risk of identity theft. The databases must also be easy to use and able to withstand the kinds of extreme demands to which they are likely to be subjected on Election Day. While the current guidance recognizes some of these challenges, it addresses the technical issues only at the highest level of detail. We urge the Commission to provide more technical detail on a broader set of issues as it further develops this guidance. Our committee stands ready to assist the EAC or to work with other members of the technical community to provide such detailed guidance.

---

[1] The testimony and bios of the committee members can be accessed at http://www.acm.org/usacm/Testimony/EAC_apr05.pdf

USE OF SOCIAL SECURITY NUMBERS

The personal and financial damage that can result from unauthorized access to or misuse of Social Security Numbers (SSNs) – a risk made all too clear by the recent spate of data breaches at large companies and the increase in identity theft – makes the use of SSNs in voter registration databases particularly sensitive and risky. Section 303(a)(5)(C) of HAVA recognizes the need to keep this information secure; however, the Act does not detail how to best protect SSNs. The committee urges the EAC to specify (1) methods or best practices for states to use in limiting and auditing access to SSN data within their databases and (2) to allow the use of SSNs only for verification purposes, not as identifiers. In any case, more detailed guidance is needed regarding steps to ensure the security and privacy of SSN data.

SECTION II, NUMBER 8 - TYPES OF DATABASES

The committee feels that the guidelines would be improved by the addition of specific guidance regarding the database options available to states. Committee members would prefer to see fairly detailed requirements or standards for both of the two major options available to states for implementing voter registration databases: namely, (1) the centralized model or (2) the distributed model, both of which are mentioned only briefly in the draft guidance.

Members of the committee are also concerned about the draft guidelines' focus on "uniform software." A better approach would be to focus on agreeing to a uniform format or schema for database content to follow. States would then have more flexibility in deciding on how to implement their own databases using an accepted, standardized data format. The committee feels that such flexibility is particularly important given the likely mix of software, hardware, network configuration, levels of IT support, and variations in expertise that one is likely to find amongst the states. Again, the committee offers to work with the EAC and others in the technical community to develop such a schema.

SECTION II, NUMBER 10 - COORDINATION WITH OTHER AGENCY DATABASES

HAVA's mandate that voter registration databases be coordinated with other statewide databases can, if not properly handled, undermine the accuracy of the voter registration data. Therefore the committee urges the EAC to pay careful attention to ensuring the accuracy of data as it develops this guidance. Knowing when and how voter registration records are created or amended or when active status is changed to inactive is important to establishing and maintaining accuracy. The committee feels that all information gathered during the registration process, including information about applications that are rejected or incomplete, should be retained for an appropriate period in order to support auditing. However, the guidance should offer direction as to how to ensure that only valid information can be used to verify a voter's eligibility. Well-managed and accurate

records will better inform citizens, voters, interested third parties, and election administrators about the implementation of voter registration rules and procedures.

The committee feels strongly that the guidelines should include more detail on the coordination of voter registration databases with other state agency databases (e.g., DMV records, death records, felony records, and so on). Such database integration represents a major potential source of inaccurate data as a person's address and legal name may differ among state databases due to differing policies among state agencies for sourcing, updating, and validating data. For example, property records may not reflect the most current addresses of the owners of record. Vehicle registration data may not reflect changes in a person's name (e.g., marriage) until a title transfer occurs.

Because automation can undermine accountability and make it difficult to maintain an audit trail, states should also be urged to resist the temptation for automated 'merges' and 'purges' of voter registration data based on matching with other state databases. In the case that such merges and purges are carried out, we recommend that that they are done with care. For example, changed, added, or deleted fields should be notated with the date and source of the change. This will make it easier for corrections to be made, as well as for databases that introduce too many errors to be identified so that their use for merges and purges can be discontinued.

SECTION II, NUMBER 11 - ACCESS CONSIDERATIONS

Another important area of consideration that the committee feels does not receive adequate attention within the draft guidance regards the levels of access of database users. The committee feels the guidance should recommend that election officials detail fine-grained permissions for users of the database. Each user should be allowed to read (or update) only those data fields that are relevant to his or her role. For example, an "eligibility-check" might allow a user to write to one field, but only read another depending on that person's role. Furthermore, the privileges should be location-sensitive. For example, a Boston official might have full privileges for voters located in Boston, and fewer privileges for voters elsewhere in Massachusetts. Privileges on other localities would be limited to determining if Boston voters had moved and registered elsewhere. We recognize that states will organize their processes differently; thus, the guidance might list sample roles and levels of privilege that are appropriate for each user.

CONCLUSION

We thank you for the opportunity to comment on this guidance. We encourage the EAC to draft more detailed guidelines focusing on making these databases secure, accurate, reliable, easy to use, and rigorous, while protecting sensitive information and minimizing the risk of identity theft. The committee's full report will be available later this year, and, as mentioned above, the committee stands ready to work with the EAC and other members of the technical community.

Members of the ACM Committee on Guidelines for Implementation of Voter Registration Databases:

Dr. Paula Hawthorn (retired database company executive), Co-chair of Study
Dr. Barbara Simons (retired, IBM Research and former ACM President), Co-chair of Study
Prof. Chris Clifton (Computer Science, Purdue)
Prof. David Wagner (Electrical Engineering and Computer Science, UC Berkeley)
Dr. Steven M. Bellovin (Computer Science, Columbia)
Prof. Rebecca N. Wright (Computer Science, Stevens Institute of Technology)
Dr. Arnon Rosenthal (Research Scientist, MITRE Corporation)
Mr. Ralph Spencer Poore (Consultant, Privacy and Security)
Ms. Lillie Coney (Associate Director, Electronic Privacy Information Center)
Mr. Robert Gellman (Consultant, Privacy and Security)
Dr. Harry Hochheiser (Computer Professionals for Social Responsibility)

For detailed bios please visit: http://www.acm.org/usacm/Testimony/EAC_apr05.pdf