ELECTRONIC PRIVACY INFORMATION CENTER

U.S. Election Assistance Commission (EAC)
1225 New York Avenue, NW
Washington, DC 20005

Agency Rule Making
Statewide Centralized Voter Registration Databases

COMMENTS
May 25, 2005
The National Committee for Voting Integrity (NCVI)

The National Committee for Voting Integrity (NCVI) is writing to offer comments to the U.S. Election Assistance Commission (EAC) as it prepares recommendations to states on the creation of a single, uniform, official, centralized, interactive computerized statewide voter registration list, as mandated by the Help American Vote Act (HAVA).

NCVI appreciates this opportunity to contribute the EAC's deliberative process regarding recommendations to states on the creation of statewide-centralized voter registration lists. We would also like to encourage the agency to make greater use of NCVI's expertise and resources as well as other computer security professionals, which should include cryptographic experts in developing recommendations to states on the creation of statewide-centralized voter registration databases.

We understand from the EAC's *Draft Proposed Voluntary Guidance on Implementation of Statewide Voter Registration Lists* that states will receive guidance on both centralized and decentralized systems. It is our collective advice to the EAC that elections must require an end-to-end concern for a wide variety of integrity requirements, beginning with the registration process, ballot construction, and continuing through vote tabulation and reporting. Several of these aspects of public elections have been discussed in hearings held by the EAC. Therefore, we would like to focus our comments to the EAC on the importance of election administration to successfully meet the challenge of creating in practice secure accessible, accurate, and reliable statewide-centralized voter registration databases. According to the Caltech-MIT Voting Technology Project report "Voting: What Is What Could Be,"[1] of the 4 and 6 million votes lost in the 2000 election,[2] the majority were attributed to problems with voter registration or polling place practices.

Because of the level of interest shown by computer technologists, media, election reform supporters, and voting rights advocates throughout the United States there is a great deal of interest in the subject of computerized voting systems. The EAC's work is greatly anticipated, which means the decisions you make will be closely reviewed and reported on by computer technologists, media, researchers, academicians, civil rights and voting rights communities.

Voter registration databases intended to be the sole source of information on eligible voters for public elections should have well defined critical requirements, by which we mean that the failure of systems to meet their requirements may result in eligible citizens who attempt to register or eligible voters who attempt to vote—being denied that right.[3] It should be made clear to states that the failure to meet these requirements may result in failures in the voter registration process and the verification of legally registered voters during an election. Statewide-centralized voter registration database critical requirements should include: adequate system reliability, data confidentiality, and system responsiveness during high volume periods.[4] For this reason, it will be important for each state to develop an effective security policy that rest first on accountability and authorization. Knowing who is ultimately responsibility for inputting, changing or deletions of voting registration information is of critical importance to the integrity of these systems. Limiting access to only those who are required to perform clearly delineate task is one component to securing and managing complex data structures.

Accuracy of voter registration lists is a vital component of election integrity. Electronic voter registration and centralized registration databases present challenges to accuracy. Knowing when and how voter registration records are created, amended, or active status is changed to inactive is important to establishing and maintaining accuracy. To maintain an accurate single centralized list of all legally registered voters should support the retention of all information gathered during the registration process. This list should include the information of those applications that are rejected, deemed to be invalid or missing vital information related to a successful registration. Keeping all records will better inform citizens, voters, interested third parties, and election administrators on the implementation of voter registration rules and procedures.

States that have well defined accountability and authorization procedures will be better able to define and establish processes to ensure the security, integrity, availability, and confidentiality of voter registration information. To make accountability and authorization procedures functional in a complex data structure, such as the one proposed will require the appropriate and correct application of cryptographic techniques. When correctly applied cryptography can assist to create authentication, integrity, and nonrepudiation of database users.

Proper application of cryptography does not rely upon keeping the way the algorithm works a secret.[5] Today this approach is unrealistic in achieving system security. Cryptography can assist with controlling who may add, delete, or change voter registration records, and who may provide final approval for large scale changes as defined by election officials. Maintaining records of those who make or approve changes to voter registration records will assist with oversight of the voter registration system.

If properly applied computers and related technology can provide many benefits that addressing the challenges identified with the management of voter registration lists. However, the development and implementation of such systems should flow from potential risks, which include: infrastructural factors, hardware malfunctions, software misbehavior, communication media failures, and human limitation in system use.[6] The areas presenting the greatest challenges relate to confidentiality, integrity, and availability, computer misuses, and security accidents.[7]

Security is vital with any computerized system, which also include those containing personally identifiable information such as the ones proposed for voter registration management. In any computer system, whether centralized or distributed, there are security threats. There are also threats to a decentralized computer systems, called distributed networks, which require periodic connection to a centralized system. Computer security should be approached as an end-to-end task that must include all parts of the system's hardware, software, computer disks, tapes, personnel, etc.

HAVA proposes the use of state drivers license bureaus to assist with the management of statewide-centralized voter registration systems. However, there may be an intent to also use public assistance records, tax records, birth records or death records as a means of managing voter registration records, which may present problems for legally registered voters. The maintenance of other state systems of personal information, including statewide drivers license systems are poor examples in many cases. In particular, state motor vehicle registration systems can be used to illustrate what NOT to do.

The computer systems managed by state departments of motor vehicles are vulnerable to insider threats, computer viruses, programming errors, and system failures. In 2003, the Maryland Motor Vehicle Administration (MVA) offices were vulnerable to a computer worm on their Windows based system.[8] This one attack disrupted operations in all 23 MVA offices located throughout the entire state. The worm took down the MVA's computers and telecommunication systems effectively shutting them down and cutting them off from all forms of remote communication. On January 20, 2004, the MVA could not process work on their mainframe computer for about an hour after opening because of a problem characterized only as a computer "glitch."[9] Either of these events occurring on an Election Day would be devastating to voters and severely undermine confidence in the outcome of the election. In a recent incident in the state of Maryland, a MVA employee was charged with conspiring with others to sell more than 150 state identification cards.[10]

If databases are linked – i.e. voter registration and driver license databases, public assistance registries, death notices, or tax records– security threats or risks in one system can affect the other system. Care should be taken to ensure that records are not altered, deleted, or amended solely on the basis of what a computer record on one system might imply about a record maintained on another system. Further, the process that allows the comparing of information on non-voter registration systems when found to be of some benefit should not use automated protocols that make changes, deletions, or additions to voter registration records without human authorization.

The security threats to statewide-centralized voter registration systems include denial of service attacks, hacking, insider threats, which could include unauthorized access, authorized access for unauthorized changes, data integrity, and social engineering threats. While some risks can be eliminated, those risks that cannot be eliminated should be effectively managed. A perfectly done computer security system can be compromised, most likely, by lack of training or inappropriate human action. The training of employees and mundane real-world procedures, such as locking of doors may be as important as expensive software.

The goal of system management should be to detect potential security problems before they occur and address them effectively. However, another goal of system management is to conduct effective evaluation of a post security failure that might allow the reconstruction of the circumstances that lead to the incident. Even in cases where a problem was not prevented it is always valuable to know how something happened even if it is in the post event phase. Post event analysis is how computer security improves and system integrity is strengthened. In the event of a security or system failure transparency will be critical in rebuilding public confidence, understanding the problem, pursuing technology solutions, improving protocols, and when appropriate the effective pursuit of criminal investigations.

It is not the intent of system architects to see a system functions in ways that are not permissible, but total control of system behavior maybe beyond the capacity of developers to manage. Therefore, it is important to develop contingency plans for those situations that might arise that threaten the application of the system for voter registration and voter access purposes.

The right to vote is the foundation of this country, carefully and clearly enumerated in our Constitution. We owe it to our fellow citizens to work openly and steadily to protect the rights of all voters. We encourage this commission to address the defects present in current voting registration systems, and work to increase the accountability and integrity of the American voting process.

Questions that should be directed to States:

1. To what extend have state computer systems intended for use in verification of or make changes to voter registration records been evaluated for their accuracy, security, and reliability?
2. How will states protect the personal information of registered voters?
3. Are states using cryptography to secure voter registration system access?
4. Have states developed written protocols that assign responsibility for access for those who can make changes or deletions to voter registration records?
5. Do states have plans that are not technology dependent should automated voter registration systems fail or experience significant problems during early voting or on Election Day?

In conclusion, the most important lesson to take from these comments is that contingency planning is important in the context of elections because there may not be a next day to make right what may have gone wrong. For this reason, policymakers and election administrators should be prepared in advance of an election in the event of an unforeseen problem. The contingencies should be realistic, well planned, and local election officials briefed on what should be done in the event of a computerized voter registration system failure to ensure an election takes place.

NCVI is available to work more closely with the EAC in its work to draft voluntary guidance to states on statewide-centralized voter registration databases.

Thank you,

MEMBERS

Peter G. Neumann, Chair * David Burnham * David Chaum * Cindy Cohn * Lillie Coney * David L. Dill * David Jefferson * Jackie Kane * Douglas W. Jones * Stanley A. Klein * Vincent J. Lipsio * Justin Moore * Jamin Raskin * Marc Rotenberg * Avi Rubin * Bruce Schneier * Paul M. Schwartz * Barbara Simons * Sam Smith

BACKGROUND

The National Committee on Voter Integrity (NCVI) was established to promote voter-verified balloting and to preserve privacy protections for elections in the United States. The Committee brings together experts on voting issues from across the country.

[1] Caltech-MIT Voting Technology Project, *supra* note 9.

[2] Caltech-MIT Voting Technology Project, *supra* note 9, at 3.

[3] Peter G. Neumann, pg 3, “Computer Related Risks,” publisher Addison-Wesley, 1995.

[4] *Id*.

[5] Bruce Schneier, page 3, “*Applied Cryptography: Second Edition*,” publisher John Wiley &

Sons, Inc.

[6] Peter g. Neumann, pg 6-7, “Computer Related Risks,” publisher Addison-Wesley, 1995

[7] *id*.

[8] Christian Davenport and Hamil R. Harris, pg. A09, “Md’s MVA Offices Forced to Shut Down,” Washington Post, August 13, 2003

[9] Staff Writer, pg. 6B, “Glitch at MVA branch offices delays some transactions for an hour, The Baltimore Sun, January 21, 2004

[10] Eric Rich, pg. B03, “Md, MVA Employee Charged in ID Card Sales, available at http://www.washingtonpost.com/wp-dyn/articles/A10710-2005Apr22.html, April 23, 2005.