



Testimony of
Wendy R. Weiser, Associate Counsel
Brennan Center for Justice at NYU School of Law
Before
The Election Assistance Commission
April 26, 2005

Good afternoon, Commissioners, and thank you for the opportunity to address you at this important hearing. My name is Wendy Weiser, and I am an attorney at the Brennan Center for Justice at NYU School of Law. The Brennan Center is a non-partisan organization that unites scholars and advocates in pursuit of a vision of inclusive and effective democracy. Toward that end, the Center's Democracy Program promotes election reforms that both eliminate barriers to full and equal political participation and are efficient to administer. Since 2002, the Center has been monitoring the implementation of the Help America Vote Act (HAVA), including the statute's database provisions.

We are very pleased that the Commission has issued its first draft Guidance on statewide voter registration databases and is soliciting input to improve that Guidance. Because the Guidance is extremely limited in scope and only begins to touch on some of the complicated issues states are facing in implementing HAVA's statewide database requirements, my remarks will focus primarily on what we believe is missing from and should be added to the Guidance. Our hope is to encourage the Commission to offer states more specific direction as to how to avoid infringing on voters' rights as they automate and streamline their voter registration lists and list management systems.

Although a statewide voter registration database can help states improve the administration of elections in a variety of ways, the primary purpose of HAVA's statewide database requirements is to ensure that states maintain a list of registered voters that is as complete and as accurate as possible. While the statute requires each state to take steps to remove duplicate records and those of ineligible voters from its list,¹ it also requires states to protect voters' rights by ensuring that "the name of each registered voter *appears*" on the list,² and that "*only* voters who are *not* registered or who are *not* eligible to vote are removed" from the list.³

¹ 42 U.S.C. §§ 15483(a)(2)(A)(ii), (a)(2)(B)(iii) & (a)(4)(A).

² *Id.* § 15483(a)(2)(B)(i) (emphasis added).

³ *Id.* § 15483(a)(2)(B)(ii) (emphasis added). HAVA further requires states to establish "[s]afeguards to ensure that eligible voters are not removed in error" from the list, *id.* § 15483(a)(4)(B), to ensure that the

Unfortunately, the current Guidance does not provide states with sufficient direction as to how they should comply with HAVA's mandates to protect voters' rights as they implement and use their statewide databases. It is imperative that the Commission provide guidance on these issues at the outset, because a poorly designed system that does not have adequate safeguards to protect voters' rights may be very difficult and costly to modify after it is constructed.

Since time is short, I will focus on the most important protections that we recommend the Commission include in its Guidance.⁴

I. Recommended Guidance for Verifying Voter Registration Information

First, perhaps the most important topic that the Guidance does not adequately address is how states should implement HAVA's verification provisions. The Guidance currently says that states should attempt to "match" information provided on voter registration applications with that in drivers' license and social security databases "for the purpose of verifying the accuracy of the information" provided by new registrants. It says nothing about what criteria should be used to determine a match or what states must do if their verification process fails to produce a match.

For the reasons discussed below, the Commission should clarify that:

- States must develop uniform, non-discriminatory, specific, and transparent matching criteria that maximize election officials' ability to find matching records.
- States may not require an exact match of all information in both databases but rather should adopt a "substantial match" standard.
- In the event a record does not produce a match, states must audit the record for errors and must employ alternative checking mechanisms.
- States must attempt to match records in all the databases with which the statewide list is coordinated, including NVRA agency databases.
- Most importantly, states may not reject voter registration applications merely because they are unable to find matching records in another database.

The adoption of these recommendations is essential if states are to meet HAVA's goal of ensuring that eligible voters are not disenfranchised as a result of administrative and other errors that may affect the matching process.

removal of any name be done in accordance with the protections of the National Voter Registration Act, *id.* §§ 15483(a)(2)(A)(i) & (a)(4)(A), and to ensure that "voter registration records ... are accurate and updated regularly," *id.* at § 15483(a)(4).

⁴ This written testimony includes more material and detail than I will provide orally at the hearing.

The need for states to develop transparent matching protocols with appropriate checks and protections flows from the difficulty in reliably matching data in two different databases, each of which records data in different ways and each of which is likely to contain errors, such as misspellings, transposed characters or inverted names.

The most infamous example of poor matching criteria is the list of suspected felons Florida developed in 2004. The state contractor that compiled that list did so by matching the names on the state's list of registered voters against the records maintained by its department of corrections. In order for a match to be found, the contractor required matching information in a variety of fields, including a field for race. The problem was that one database had a category for Hispanics and the other did not. The result was a list that systematically excluded Hispanics.⁵ Similarly, a matching protocol that does not check for transposed first and last names may systematically fail to find matches for Asian-Americans.

Regardless of how good a state's matching protocols and checks are, errors are inevitable. It is therefore essential that the Commission make clear that states may *not* refuse to register a voter whose information it is unable to match. In fact, for the reasons laid out in a footnote to my testimony, this rule is compelled by HAVA.⁶

Although most of the states we have surveyed indicate that they will not reject voter registration applications merely because they do not produce a match with drivers' license or social security databases, several states say that they will. Not only would this violate HAVA, but it would also lead to mass disenfranchisement of eligible voters. New York City's recent experience suggests the potential scope of the disaster that would ensue. Last September, the city's board of elections sent 15,000 registration records with

⁵ Indeed, out of 48,000 "suspected felons" in a state with a large Hispanic population, only 61 were Hispanic. In contrast, 22,000 were African-American. While Florida used this match protocol to remove citizens from its list of registered voters, we are concerned that a similar protocol in the verification process could be used to prevent eligible voters from being added to the list or from being exempted from HAVA's identification requirements.

⁶ HAVA requires states to adopt safeguards so that eligible voters are not denied the franchise as a result of administrative errors. *See, e.g.*, 42 U.S.C. §§ 15483(a)(4)(B) & (a)(2)(B)(ii). A system that deprives citizens of the right to vote when the state cannot match their registration information is simply not a sufficient safeguard, given the large error rate.

In addition, a rule rejecting voter registration applications for failure to produce a match would be inconsistent with other provisions of HAVA. For example, HAVA § 303(b)(3) exempts first-time voters who register by mail and whose identifying numbers the state matches with an existing state record from HAVA's identification requirements, while preserving their right to vote at the polls on election day. 42 U.S.C. § 15483(b)(3). This provision clearly contemplates that the state will not be able to match all of the identifying numbers provided by applicants for voter registration and that those applicants will still be able to register to vote. Indeed, HAVA's identification requirements are triggered only when a state *cannot* match the voter's registration information with an existing state record. Those requirements would make no sense if such voters were not registered in the first place. Further, a new registrant whose numbers do not match and who fails to provide identification either with their voter registration application or at the polls on Election Day is entitled by HAVA to vote by provisional ballot. 42 U.S.C. § 15483(b)(1)(B). That right would be completely obliterated if the state refused to register voters whose identifying numbers it fails to match.

driver's license numbers to the state department of motor vehicles for verification. The department flagged 2,959 of those records – about 20% – as listing driver's license numbers that did not match any numbers in the department's database. Fortunately, the city board of elections undertook a massive audit of its database by reviewing the scanned original of each registration form that did not produce a match. It found that the driver's license numbers on 2,951 of those records – 99.7% – were incorrectly entered by election officials. Had the city rejected those applications for failure to produce a match, close to 20% of new registrants who had supplied driver's license numbers would have been disenfranchised as a result of typographical errors by election officials. This is precisely the type of harm that HAVA was intended to prevent.

Although list audit procedures should be required, that will not entirely solve the problem. For one thing, it will be impossible for election officials to catch all errors by manually reviewing thousands of new registration records, often in very a short time period. More importantly, audits of the records in the statewide database will not catch errors in the matching databases. The Social Security Administration estimates that at least ten percent of the information obtained when attempting to match records with its database will be inaccurate. It is unacceptable for a state to make a potential voter's access to the franchise turn on these odds.

II. Recommendations for Adding and Updating Voter Registration Information

Second, the Commission should adopt more detailed guidelines to make sure that new voter registration applications and updates to existing voter registration records are accurately reflected in the statewide database in a timely manner, as required by HAVA.⁷ Specifically, the Commission should recommend the following rules:

- Registration forms submitted to state election officials or at voter registration agencies must be processed on an expedited basis, even before they reach local election officials.⁸
- Registration records should be electronically transmitted from all agencies that accept registration forms to prevent the loss of data and to reduce the risk of error. This can be facilitated by electronic links and interactive connections to the databases of those agencies.⁹

⁷ See 42 U.S.C. §§ 15483(a)(1)(A) & (a)(4).

⁸ Although the Guidelines currently reiterate HAVA's explicit requirement that local election officials enter new registration data on an expedited basis, they say nothing about how quickly the state must process registration applications before they reach local officials. The rule we recommend follows from HAVA's requirement that "the chief State election official *shall* provide such support as many be required" to ensure that voter registration information is input by local election officials on an expedited basis. 42 U.S.C. § 15483(a)(1)(A)(vii). Pursuant to this provision, state election officials have an obligation to ensure that applications are processed quickly from the time they are received by *any* state official, not only from the time they are received by local election officials.

⁹ The electronic transmission of registration records should nonetheless be accompanied by physical transmission of the application forms to appropriate election officials. The original applications should be maintained as a backup record of the registration of each voter.

- The Commission should require periodic audits of the information input in the voter registration database, including by checking the electronic records against the original paper applications.
- To the extent possible, records in statewide databases should be updated and accessible in “real time.”¹⁰
- The Commission should more explicitly require that database coordination be used not only for the purpose of verifying voter information but also for the purpose of correcting, supplementing, and updating the information in voter registration forms and records. All available databases should be consulted for this purpose, including those of social service and disability agencies.
- Where applicable, the Commission should encourage states to coordinate their voter registration databases with those maintained by the department of corrections to ensure that the registration list reflects the automatic restoration of rights of persons who complete their incarceration, parole, or probation.

III. Recommendations for Removing Voter Registration Records and Protecting List Security

Third, the Commission should adopt clear guidelines regarding how states can fulfill their obligation under HAVA to establish “safeguards to ensure that eligible voters are not removed in error from the official list of eligible voters.”¹¹ To protect against erroneous purges, we recommend that the Commission endorse the following rules:¹²

- States should establish multiple and redundant checking systems before concluding that a record potentially is a duplicate or belongs to an ineligible voter.
- States must develop uniform, non-discriminatory, and transparent standards for determining when a registration record is subject to removal from the list.
- Before removing any name from the computerized list, states must notify the voter¹³ and provide her an opportunity to correct any errors or omissions in her

¹⁰ See 42 U.S.C. § 15483(a)(1)(A)(v) (all state election officials must “obtain *immediate* electronic access to the information contained in the computerized list”).

¹¹ 42 U.S.C. § 15483(a)(4)(B).

¹² For more detailed recommendations on how states that disenfranchise persons with felony convictions should conduct purges of those persons from their lists, please refer to ACLU, DEMOS & RIGHT TO VOTE, PURGED! (Oct. 2004), *available at* <http://www.aclu.org/VotingRights/VotingRights.cfm?ID=16845&c=167>.

¹³ Notification should be made by a certified, forwardable letter to her last know address, along with a postage pre-paid response card.

record, including errors caused by election officials.¹⁴ This requirement follows from HAVA's prohibition against removing the records of any eligible voter, coupled with the fact that there is no reliable method of generating accurate lists of ineligible voters or of duplicate records. This requirement is also essential to ensure that citizens are not denied their fundamental right to vote without due process of law.

- States may not purge voters' names or engage in organized list maintenance activities within 90 days of an election (other than with respect to individuals who become ineligible during that period).

HAVA also requires that states implement technological security measures to protect against unauthorized access to the computerized list.¹⁵ This includes protecting against unauthorized list transactions, including transactions that result in purging the names of eligible voters. Toward that end, the Guidance should include the following security measures:

- Statewide databases should keep electronic records of all database transactions, including transactions to remove names from the list. These electronic records must indicate the date and time of each transaction, the identities of the persons who removed or modified records, the identities of the persons who authorized the transaction, and the reason any record was removed from the list.
- The database must also be capable of generating reports of all such transactions to facilitate state oversight and public monitoring of list maintenance activities.
- States must adopt security protocols and authorization procedures to prevent unauthorized persons from accessing, destroying, or tampering with voter records. The database should be constructed to permit different layers of access and authorization so that only authorized individuals may view records and perform specified transactions. The security protocols and access rules must be made public.
- The database should prevent any one user, acting alone, from removing names from the list. The removal of any record must be authorized by at least two officials (preferably with different political affiliations and at different levels of government). For example, if a state election official flags a record for removal, that record should remain on the list until the decision to remove is confirmed by an appropriate local election official.¹⁶

¹⁴ This recommendation is similar to that made by the Midwestern Legislative Conference of the Council of State Governments in its August 2002 report (recommending that “[p]rocedures governing the purging of duplicate registrations should include sufficient notice to affected voters and an opportunity to correct errors in a timely fashion”).

¹⁵ 42 U.S.C. § 15483(a)(3).

¹⁶ A similar protocol allowing county officials in Florida to reject the state's recommended purges mitigated the discriminatory effects of the state's infamous 2000 purge.

IV. Recommended Guidance Concerning HAVA's Privacy Protections

Fourth, the Commission should adopt more specific guidelines for how states must comply with HAVA's privacy requirements.¹⁷ The development of statewide voter registration databases that are coordinated with other state databases creates a substantial risk that confidential information about voters may be accessed by unauthorized persons and for improper purposes. This could leave many voters susceptible to identity theft or other injuries. It is therefore essential that states adopt strong protections for voters' privacy and security, especially in connection with the integration of databases. These protections must be specified at the outset, because they may implicate database design. Important protections that should be included in the Guidance include the following:

- States must adopt protections to prevent access, to all but a small number of authorized persons, to a voter's sensitive personal information, such as her social security or driver's license number or the information provided by domestic violence victims. The database should be capable of masking this information, which should be used only for verification purposes.
- More generally, states must adopt strict protocols for access to voter records, including protocols to ensure that only authorized persons may view certain information and perform certain tasks.
- In addition, states must prevent private information contained in the voter registration database from being viewed by users of other databases to which it is linked; conversely, states must prevent election officials from accessing private information from those other databases.

V. Recommended Guidance on Voters' Access to Their Registration Records

Fifth, the person in the best position to ensure the accuracy of the information in a voter's registration record is the voter herself. A computerized statewide registration list makes it easier to allow citizens to monitor their registration status and check the accuracy of their records so that errors may be corrected before Election Day. The Commission should adopt a guidance recommending that states enable each voter to access or view her own registration record, preferably through an internet-based copy of the database registration record. This public portal should have strong security protocols to prevent persons other than the voter from viewing the confidential information in her record. A computerized polling place finder for voters should also be recommended.

VI. Recommended Guidance Concerning Additional Functions of Database

Finally, the Commission should adopt recommendations concerning additional functions and uses of statewide databases.

¹⁷ See 42 U.S.C. §§ 15483(a)(3), (a)(5)(C) & (a)(5)(D).

Although HAVA does not require states to use their databases for election management activities other than registration list management, a well-constructed database can be used to assist states in virtually all aspects of election administration, including managing and keeping track of absentee and provisional ballots, printing ballots, assigning precincts, and tracking poll workers. We hope that the Commission will encourage states to develop databases capable of a variety of election management functions. This will promote better run elections and will save states substantial costs over time.¹⁸

In addition, HAVA requires that the statewide database “serve as the official voter registration list for the conduct of all elections for Federal office in the State.”¹⁹ To comply with this provision, states should make the database itself – the only “official” list – available at polling places on Election Day. Polling place access to a searchable database will reduce the number of eligible and registered voters whose names cannot be found on the list, preventing disenfranchisement as a result of the difficulties of searching a printed list, reducing the number of provisional ballots, and enabling poll workers to determine if a voter is in the correct polling place. The Commission should therefore recommend that states provide each polling place with electronic access to the statewide database (or a searchable copy of the database).²⁰

Conclusion

One of the main impetuses for the enactment of HAVA was the discovery that as many as three million eligible voters were denied the franchise in the 2000 election because administrative errors prevented their names from being found on the states’ voter registration lists. Computerization of those lists will not eliminate registration processing errors. It will, however, make it easier for states to update and correct registration records and to better protect voters against the possibility of disenfranchisement due to errors. We urge the Commission to provide the states with better guidance as to how they should protect voters’ rights as they implement HAVA’s database provisions, including by adopting the recommendations I have made today.

Thank you.

¹⁸ Indeed, it is not unlikely that future federal legislation will require databases to be used in this manner. A number of states and localities already have sophisticated election management systems tied to their voter registration databases.

¹⁹ 42 U.S.C. § 15483(a)(1)(B).

²⁰ This is generally done via laptop computers.