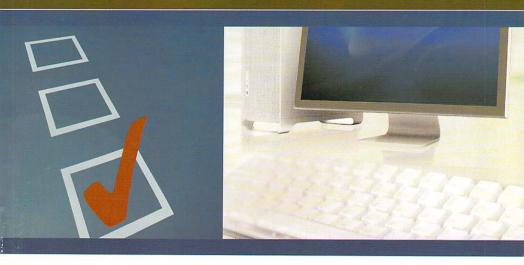# THE DATABASE DILEMMA:

Implementation of HAVA's Statewide Voter Registration Database Requirement

BEST PRACTICES BOOKLET

The Advocates Guide to the Public Policy Issues

Appleseed

Sowing Seeds of Justice Through Law

LATHAM&WATKINS LLP

Appleseed — Sowing Seeds of Justice Through Law | **The Database Dilemma**

Acknowledgements

Table of Contents

Executive Summary

Election problems associated with the 2000 election were a catalyst for Congress to pass the Help America Vote Act ("HAVA") in 2002. HAVA attempted to overhaul many aspects of the voting process in order to ensure that every eligible American was given the opportunity to have his or her vote counted. The Act established federal requirements mandating that states issue provisional ballots, increase access for disabled voters, and create statewide computerized voter databases, among other things. Many of these requirements have not yet been fully implemented. Election Day 2004, in particular, demonstrated that HAVA's mission is a work in progress. Voters endured erroneous purges, missing absentee ballots, long lines, poll closings, and contested provisional balloting.

In many regards, HAVA left states with a great deal of discretion in terms of how they comply with HAVA's requirements. To assist the states, Congress authorized the United States Election Assistance Commission ("EAC") to issue voluntary guidance interpreting the provisions of HAVA and recommending specific means by which HAVA may be implemented. The states, however, may fulfill HAVA's mandate through provisions even more protective of the rights of voters than EAC guidance might suggest – and several states have already chosen to do so.

One of HAVA's requirements is that each state must establish a single system for storing and maintaining all the voter information for each eligible voter in the state by January 1, 2006. This system – the statewide "Database" – must be "defined, maintained, and administered at the state level." This requirement was intended to deal directly with voter registration problems and, by extension, complications with provisional voting, voter fraud, and general disenfranchisement.

The purpose of this manual is to offer guidance to each state in developing its Database. The requirements for the Database under HAVA are broad but clear: states must ensure that "the name of every eligible voter appears" in the system, that only the names of ineligible voters are removed from the system, and that "eligible voters are not removed in error." Beyond that, states have a fair degree of discretion in how the Database is constructed. In developing this manual, we identified six critical steps to building a successful Database. These six steps are explained in relation to their statutory requirements under federal law, various specific policy concerns, and the lessons learned by states that have already implemented Databases. In forming our recommendations, we sought to promote a variety of overarching goals, including voter enfranchisement, the reduction of error, the limitation of concern regarding improper registration, and the protection of individual privacy and data security.

For each critical step to building a successful Database, we have included specific policy recommendations for Database implementation: i.e., "Best Practices." However, we also recognize that because state administrators operate under resource constraints it is not always possible to implement

Executive Summary continued

the best solution to some of these issues in the short term. To that end, where possible, we have identified alternative choices that can be made in light of these constraints, but that are nonetheless sub-optimal to our "Best Practice" recommendations. These alternative choices are labeled "Avoid Where Possible." Our acknowledgment that administrators may be forced into such choices on an interim basis should not be construed as an endorsement of these practices.

During this period of implementation, states have a critical but exciting moment of opportunity to create a Database that makes voter registration easy and available, reduces the risk of ineligible votes and erroneous purges, and ultimately increases confidence in democratic outcomes, and to do so in a way that is efficient and cost-effective to administer. We hope that this Best Practices Manual is both encouraging and instructive to states in this important endeavor.

How to Build a Database

Outsourcing

The first decision a state must make in building a Database is whether to outsource the development and maintenance of the Database or to undertake these tasks with in-house personnel. State and local governments, like private-sector companies, already outsource a variety of discrete projects. For example, most credit card companies outsource the majority of their processing so that virtually every step is outsourced, from the time a card is swiped to the time the monthly statement arrives. Outsourcing a voter registration Database has some elements in common with these other contracts, but is also subject to some unique considerations. For example, while there are certainly privacy and security concerns over credit card information, there may be even greater concerns when it comes to an individual's voter history and the kinds of personal information stored in the Database.

Procurement

States should make sure that they are not held hostage to their original vendors in perpetuity, and that they maintain the freedom to contract with different vendors, or with none at all. In order to do this, states must make sure that any contract provides that the state will own all of the software that a vendor develops to create the Database. In the alternative, states could accept perpetual licenses to necessary software, provided they have the right to operate and maintain the software and to engage third parties to do so. In any event, states should own all data housed in the Database. States should strongly prefer vendors who use common platforms and computer code. This way, if a state chooses to work with a different vendor, or if the state decides to make changes at a later point, a vendor can make those changes using the original source code and not be tethered to one particular vendor.

Integration

The Database requires standardized data formats across state election offices and preferably also across other agencies, such as the Department of Motor Vehicles ("DMV") and the Social Security Administration ("SSA"), which are connected to the Database. Because other databases for non-election-related state agencies contain information pertinent to voter registration, that information should be used to verify and supplement information given by voter applicants. Additionally, collateral state agencies should receive voter registrations from applicants directly and be able to ensure that they are entered into the Database in a reasonable amount of time. To ensure that other state agencies can access the Database, the data format and computing platforms of the agencies' Databases should all be compatible.

Voter Data

States should think carefully about the amount and type of voter data they store on the Database. This question is significant for several reasons. On the one hand, keeping the amount of data on voters to a minimum will ensure that if the Database security is ever breached, no extraneous personal information will be available. On the other hand, requiring more fields of data on

How to Build A Database continued

voters to be matched before a voter is removed as a duplicate will reduce the number of erroneous purges. Additionally, identifying voters by a unique identifying field or combination of fields will limit the confusion arising from voters with the same name, or voters who change their name.

Transparency.

States must strike the right balance between keeping Database information private and secure, but also available for the purposes of auditing and oversight. Striking that balance means recognizing that different forms of data have different degrees of vulnerability. For example, the source code used to build the Database should not be made publicly available because if it is disrupted it can have a catastrophic effect on the information stored. Placing the source code in escrow will allow independent review of the code, thereby protecting against internal fraud and manipulation and promoting transparency. Additionally, escrowing archival copies of the Database information will preserve an audit trail of changes made to voter records.

> ***Do It Right, Do It Once.*** The requirement that states develop a Database by January 1, 2006 is a once-in-a-generation opportunity to overhaul the voter registration process. Because of the technical choices involved, once a state follows through with the Database it will be difficult, if not impossible, to go back and make discrete changes. For this reason, it is vitally important for state legislators to make the right decisions, right now.

Procuring External Services

Statutory Requirements:

- "The specific choices on the methods of complying with the requirements of this title shall be left to the discretion of the State." 42 U.S.C. § 15485

- "The appropriate State or local official shall provide adequate technological security measures to prevent the unauthorized access to the computerized list established under this section." 42 U.S.C. § 15483(a)(3)

Concerns and Solutions:

- **Whether to Procure Services from an External Supplier:** States should do a thorough and realistic assessment of costs and risks of performing services in-house. This includes comparing the availability of appropriately skilled staff, equipment, software and other required resources with the costs and risks of procuring the services from an external services provider.

- **Transparency:** States should ensure that there is no less transparency or accountability for the services performed on the Database by an external service provider than if the services were performed in-house.

- **Understand What You're Buying:** In order to avoid unexpected charges, states should determine at the outset the exact and full scope of the services needed as well as any other requirements that may drive costs, articulate them clearly in the RFP and include them in the contract.

- **Security and Privacy:** States should ensure that the necessary system security and privacy features are designed into the Database. Importantly, states also should ensure that the systems and networks that the service provider uses to perform Database services, as well as its operational procedures, facilities and staff, meet security and privacy requirements on an ongoing basis.

Procuring External Services continued

Recommendations

Transparency:

- **Best Practice:** Require public disclosure of the owners of the service provider as well as the other principals involved in providing the services, which may require disclosure of multiple layers of ownership. Require prompt notification of any changes. Negotiate broad audit rights and the right publicly to disclose audit reports.

- **Never:** Sign a contract with an entity whose ownership is not known to the state or where the state has no right to audit the service provider's operations and performance of the services.

Predictability of Costs:

- **Best Practice:** Where volumes of processing, work or other resources consumed are expected to vary over time, seek volume-based pricing with fixed unit prices that are agreed to before the contract is executed. If the contract is for multiple years, include a benchmarking clause to ensure contract prices stay in line with the market.

- **Avoid Where Possible:** Time-and-materials compensation (e.g., hourly or full time-equivalent) or other compensation methods that shift to the customer the risk of the service provider's inefficiencies, mistakes or underestimating the cost to perform. Avoid minimum revenue or other commitments and, where volume-based prices apply, base charges.

- **Never:** Agree to "cost-plus" compensation exclusivity to the service provider, or for the service provider to perform "due diligence" after signing the contract with the result that prices may increase.

Commitment to Timeline and Quality:

- **Best Practice:** Include objective service measures and negotiate credit for faiure to meet goals. Include consequences for failing to meet critical milestones.

- **Avoid Where Possible:** A mere contractual commitment to meet critical milestones and service levels.

- **Never:** Agree that the vendor's obligation is to use "commercially reasonable efforts" to perform the services, meet deadlines or achieve service levels, or that service levels are only "targets" or "objectives." Never leave service levels or service credits to be agreed after signing the contract.

Scope and Accountability:

- **Best Practice:** Have the service provider commit to deliver a defined output. State that the scope includes any services that are implied. Clearly delineate responsibility so that the owner can be held accountable.

- **Avoid Where Possible:** Obligating the service provider only to perform an enumerated list of tasks, functions, responsibilities, etc., with the result that anything omitted from the list is the state's responsibility to perform or pay to have performed.

- **Never:** Fail to have a robust, clear statement of the service provider's scope, including deliverables, specifications for deliverables, and service levels.

Issue Analysis

Context

State election officials have an array of services relating to the Database that they have to decide whether to perform in-house or to engage an external service provider to perform. The bulk of these services are IT in nature and relate to the design, development, implementation, operation and maintenance of the Database. However, other services relate to business processes. The discussion below addresses the procurement of external services generally and, except where otherwise noted, applies whether the services are IT in nature or not. Where any particular point relates to a particular type of service or particular service supply model, that is noted below.

Utilizing Other Agencies' IT Expertise

Historically elections agencies have not had as much experience in building in-house IT resources, undertaking IT projects, operating and maintaining systems or managing external service providers as compared with other state agencies. Exceptions of course include elections agencies that have already implemented statewide Databases, and elections agencies have become more savvy in recent years with the advent of electronic voting machines. State election agencies should draw on the accumulated knowledge of other state agencies that have had more experience as users of IT systems and buyers of external services.

Procuring External Services continued

In-House or Use an External Service Provider?

Issues to consider in whether to perform services in-house include: whether staff with the requisite resources exist in-house; whether other resources exist and are available, including hardware, software and network capabilities; the ability to manage internal staff and resources adequately, including being able quickly to implement and to meet deadlines; retaining control of staff and other resources; and possible lower cash outlays for out of scope requests and speed of response to new requests.

Issues to consider in whether to engage an external service provider include: time and cost for procurement and negotiation of a signed contract; properly structuring and negotiating the contract to deliver on expectations; risk that the service provider will fail to perform; lack of control over budget; access to skilled personnel; access to newer technologies and better methodologies; greater likelihood of quicker implementation; converting fixed costs to variable costs; and more objective and transparent assessment of performance, and corresponding increased accountability, including as a result of service credits for service level failures and liquidated damages for failure to meet deadlines.

Once the choice is made to outsource Database development and/or services, states should keep the following issues in mind.

Transparency and Integrity

Because of the sensitivity of the personal information to be housed in the Database and the overarching need to maintain transparency and integrity in the elections process, even greater care must be taken in the choice of service providers that will design, build, operate, maintain or otherwise have access to the Database or the information it contains. As mentioned above, the ownership of the service provider should be disclosed as well as the identity of key managers and other decision makers who will be involved in the performance of the services. There should be an obligation promptly to inform the state of any changes in the foregoing, and the right for the state to terminate the services upon a change in ownership or remove any particular individuals from the services for good cause. States should have permissive audit rights in order to maintain transparency and integrity in the discharge of government functions. Audit rights are not limited to financial matters, but should extend to inspections of any operations, systems or facilities used by the service provider (whether it owns them or not) to perform the services. The state should have the right to use outside auditors or subject matter experts, such as IT specialists to conduct penetration and other security tests on the systems and networks used in performing the services. The state should have the right to disclose publicly the findings of any audits or inspections. The service provider should be obligated to remedy any deficiencies as soon as possible. The state should require its contractors to avoid any actual or apparent conflict of interest, including active roles in partisan activities either by the contractor or its managerial staff.

Don't overlook occasional or episodic requirements

In the context of the Database these may include: training of temporary, additional staff or volunteers during election cycles; more quickly applying updates to Database records and more frequent archival of back-ups of the Database as election day nears; increased network requirements on and around election day to connect all the polling stations and possibly to increase availability and reduce response time for better system performance; and increased service provider staffing to answer questions and provide support, including more technical staff on-hand to address immediately any operational or performance issues with the Database on election day. Moreover, if it is not affordable to have a real-time, fully-mirrored back-up system all of the time then make sure that it is possible to implement this redundancy for a finite period during election cycles, especially around election day.

Security and Privacy

Security is a particular issue when contracting with an external service provider for services related to voter registration information. Accordingly, states should carefully examine the security of the service provider's systems and networks, processes and operations, facilities, and even service provider staff who will perform the services or have access to the Database. Protocols should be put in place for levels of access, and the state may consider retaining responsibility for issuing and managing passwords to the Database. Means for detecting and procedures for notifying election officials immediately of any unauthorized access to the Database should be instituted. These may dovetail well with designing and constructing the Database to retain an audit trail of any additions, deletions or changes to records in the Database (including the identity of the user and time/date stamp). Operational processes should also be considered. For example, some of the recent disclosures of personal customer information have been as a result of back-up tapes being lost or mishandled in transit to disaster recovery sites. All back-ups should be done electronically. All security requirements should apply equally to any subcontractors performing other than incidental services.

Pricing

For fixed scopes of work (e.g., designing and implementing the Database), fixed prices should be sought. However, when services vary on an ongoing basis, volume-based pricing according to agreed, fixed unit prices should be used. Any non-ongoing events that are reasonably likely to occur, or recur, should be considered within the scope of the RFP and priced in the bids at proposal time to leverage competitive pressures. The freedom to choose a lower priced provider or to perform the work in-house is key to maintaining some threat of competitive pressure on pricing for out-of-scope work after the contract is signed. This will not be possible if an exclusivity commitment, or other minimum commitments that have similar effect, is given to the service provider. Accordingly, these should be avoided. To avoid any indirect restraints on the ability to give out-of-scope work to a third party or perform it in-house, states should obligate the service provider to cooperate with any third party or in-house resource, including allowing them to interface with the service. The contract should

Procuring External Services continued

state that there are no amounts payable to the service provider other than the prices stated in the contract. Any exceptions must be agreed to and listed in the contract.

Importance of Open Architecture; IP Rights

From the start, services should be designed using open architectures with generally commercially available applications, tools and utilities. This will allow states to smoothly transition services to another provider, if desired. For any preexisting items that are proprietary to the vendor and for which a generally commercially available replacement cannot be readily substituted at little cost, the service provider should give the state a perpetual, fully paid-up license. This license should include the right for the state to have other service providers use such item solely for the benefit of providing replacement services to the state. The state should own or have a free, unfettered license to any code or modifications to code specifically developed for the state. In any event, states should own all data in the Database and service providers should have no right to continue to use the Database after the end of the contract term.

Subcontractors

It is not uncommon for service providers to utilize one or more subcontractors. States should require approval for the use of any subcontractors initially, retain the right to have them removed at any time for good cause, and be able to approve any replacement subcontractors or second level subcontracting during the term. All obligations applicable to the prime contractor should apply equally to each subcontractor as if it were the prime contractor, unless otherwise agreed. This should include security obligations, obligations relating to staff (including the ability further to subcontract), audit rights and intellectual property rights to code and data.

'Back End' Transition Issues

Any agreement for the performance of services on an ongoing basis should contain robust obligations on the service provider to enable a smooth transition when the relationship with that service provider ends. This should include the smooth transition of any or all of the services in-house or to one or more different service providers. The incumbent service provider should be obligated to provide whatever information or assistance is required in order to ensure a seamless transition.

COLLECTING DATA AND INTER-AGENCY INTERCONNECTIVITY

Statutory Requirements:

- The Database "shall be coordinated with other agency databases within the State." 42 U.S.C. § 15483(a)(1)(A)(iv)

- All voter registration information given to any local election official "shall be electronically entered into the computerized list on an expedited basis at the time the information is provided." 42 U.S.C. § 15483(a)(1)(B)(vi)

- The chief State election official shall "enter into an agreement [with the DMV] to match information in the database . . . with [DMV information] to the extent required to enable each such official to verify the accuracy of the information . . . ." 42 U.S.C. § 15483 (a)(5)(B)(i)

- The SSA shall develop methods to verify voter information of applicants "for whom the last 4 digits of a social security number are provided instead of a driver's license number." 42 U.S.C. § 15483(a)(5)(C)

- Each state "shall determine whether the information provided by an individual [on a voter registration application] is sufficient" to meet the federal requirement. 42 U.S.C. § 15483(a)(5)(A)(iii)

Concerns & Solutions:

- **Efficiency:** Coordination with other state agencies allows voter registration information to be entered efficiently into the Database, saving states and local governments significant time and money.

- **Accuracy:** Coordination with other state agencies will help ensure that voter information has been properly entered into the Database.

- **Voter Enfranchisement:** Coordination with other state agencies increases the number of opportunities for voters to register, verify, and update their voter information.

- **Fraud & Error:** Increasing the number of persons with access to the Database increases the potential for fraudulent or accidental registration entries and purges.

- **Privacy:** Connecting state agencies to the Database could permit greater access to private information regarding driving, voter, and social security information.

Data and Interconnectivity continued

Recommendations

Agency Coordination:

- **Best Practice:** Coordinate Database with all relevant state agencies to ensure that missing voter information can be supplemented and existing information can be verified to allow for maximum voter enfranchisement.

- **Never:** Coordinate the Database only with the DMV.

Connection between Agencies and Database:

- **Best Practice:** Voter registration applications, supplemental information, and official verifications are electronically transferred from coordinating state agencies to the administrators of the Database in real time via a secure encryption protocol.

- **Avoid Where Possible:** Voter registration applications, supplemental information, and verifications are transferred from coordinate state agencies to the administrators of the Database in "batches," so that Database updates occur no later than five (5) days after information is received, and on a daily basis as the registration deadline approaches.

- **Never:** Paper transfer of voter registration applications, supplemental information, and verifications from coordinate state agencies to the administrators of the Database.

Additionally:

- The state's chief elections official should promulgate clear and binding standards for interaction by government personnel with the Database.

- The data format and computing platform of the Database should be compatible with local agencies, such as the DMV and Department of Social Services ("DSS").

- Voter registration information sent from other state agencies should be electronically transmitted to election officials, who can then easily approve updates to the Database itself.

Issue Analysis

Implementing an Electronic Interface

Creating an electronic interface between the state body responsible for elections and other state agencies not only achieves a more accurate and up-to-date voter registration system, but also encourages voting by generating more opportunities for people to register to vote. While potential voters should currently be able to register at their state DMV and other state agencies, their information is often transmitted on paper forms, which are easily lost or destroyed. Creating an electronic interface between local agency databases and the state elections authority for registration purposes would reduce the number of lost or mistyped registrations because the registration information would automatically be entered for quick review and direct input into the Database. The electronic interface would also ease the process for voters to update their voter information when they change their address or other important information at the DMV or other agency office. Creating an electronic interface where voters can request changes to their personal information for all state agencies in one stop would encourage efficient voter registration and create a more thorough and accurate record of voter information. The end result would be more trustworthy elections and possible cost savings for state and local governments.

Preventing Misconduct

While an electronic interface would bring many benefits, it can also create privacy and misconduct concerns which arise when an increased number of people are given access to voting records. These concerns can be reduced by implementing measures to ensure the protection of voter information and requiring that the actions of local election boards be monitored by the public. In order to reduce the potential for improper manipulation of voter data, any interaction with the Database – whether it is adding the registration of a first time voter, or deleting the old address of someone who just moved – should be recorded in the Database and archived at least until the conclusion of the following election cycle. This will ensure that the actions of unauthorized hackers are tracked, and that the actions of local election officials do not go unchecked; in general, it will protect against fraud and abuse by those who interact with the Database. Additionally, the state's chief election officer – usually, the Secretary of State or Attorney General – should promulgate clear and binding standards for authorized interaction with the Database. Failure to comply with these procedures can be used as evidence, inter alia, for resolving any voter registration disputes.

Protecting Confidential Information

Because many different agencies will be able to access information about individuals through the electronic interface, ensuring privacy is an important goal in the development of the Database. Information shared on the electronic interface should be limited to what is necessary to develop the voter registration system and different privacy protections should be put in place to ensure that only

Data and Interconnectivity continued

the appropriate people are using only the appropriate information for only the appropriate ends. Some information – such as a voter's driving record – should not be transmitted via the electronic interface at all. Moreover, the amount of information transmitted over the electronic interface will vary depending on the type of voter registration entry. For example, for a new voter registration entry, all registration information must be transmitted on the electronic interface. In contrast, for a simple correction to a voter registration entry, such as a change of address, it is unnecessary for all voter information to be re-transmitted. Both the benefits and concerns of the Database are increased with the number of local agencies that are connected. As such, states should make an individual assessment of the number of agencies whose access would benefit the Database, but should also be careful that the connected agencies use the electronic interface solely to register voters and do so in such a way that privacy and fraud concerns do not outweigh the benefits of the agency's connection.

Develop Data Transfer Protocols

To maintain the integrity of the Database, it is critical that the state have clear protocols for the transfer and processing of data. States should aim to create a system where voter registrations are electronically transferred (1) in real time and (2) via a secure encrypted protocol. This means that a local government official must log into a secure system and type (or approve electronically transmitted copies of) the voter's information, which can be saved into the system immediately. For state administrators without the funding or capability to create this kind of real-time system, the state should set a deadline when voter information must be transferred to the system after it is received (such as one business day).

Data Approval

Because an increase in the number of people who access the Database creates more opportunities for data to be accidentally or purposefully deleted or changed, only certain specified state or local election officials should be granted the authority to enter or update voter information directly on the Database. Therefore, all new or updated registration information sent from coordinate state agencies to the Database should be held electronically in an "electronic queue" for election officials – those with the ultimate authority to verify and accept entry of the voter registration information – to approve, before any change is made in the Database itself.

Model State Practices

- North Carolina has implemented automatic transfer of DMV registrations into county Database systems, eliminating data entry by local election officials for approximately 60% of new registrations. This efficient practice allows local election officials to spend time verifying or approving the data rather than performing data entry tasks. This system also promotes accuracy by preventing data entry errors from going unchecked and the loss of paper applications. Additionally, by eliminating the delay caused by use of paper form registration, it reduces the number of provisional ballots that must be cast.

- Arizona currently allows full online voter registration through an electronic interface between the DMV and the County Recorder in charge of local elections. The online voter registration system utilizes information stored in the DMV database, including electronic signatures, to allow residents with Arizona driver's licenses or IDs to register online.

Unique Identifying Numbers

Statutory Requirements:

- HAVA requires that each state assign a "unique identifier" to each registered voter. 42 U.S.C. § 15483(a)(1)(A)(iii)

- To the extent that a state assigns an identifying number to each individual without a driver's license or social security number, that assigned number shall also be the "unique identifier." 42 U.S.C. § 15483(a)(5)(A)(ii)

Concerns & Solutions:

- **Efficiency:** Because election officials can more clearly identify duplicate registrations when sorting voters by a unique identifying number, the unique identification requirement makes the Database more efficient, saving states money.

- **Security:** Use of unique numbers can help officials identify ineligible voter registrations and remove them before Election Day.

- **Confusion:** Using a combination of identifying numbers, rather than one unique identifier, is generally confusing and can make it more difficult for election officials to identify voters and purge duplicates.

- **Privacy:** Through mistake or fraud, voter registration lists may become publicly available. Identifying numbers that are based on a voter's driver's license number or social security number can create privacy concerns.

Recommendations

Unique identifying number:

- **Best Practice:** States affirmatively issue a unique identifying number to each voter, developed specifically for Database purposes.

- **Never:** States rely only on a identifying number developed for other purposes, such as a driver's license number or social security number.

Unique Identifying Numbers continued

Consistency:

- **Best Practice**: A voter's unique identifying number remains the same as long as the voter lives in the state.

- **Never:** A state changes a voter's identifying number if the voter moves to a different county within the same state.

Voter enfranchisement:

- States should make explicit that no voter's registration application, update of registration information, or actual vote will be rejected because the applicant fails to provide his or her unique identifying number. If an application lacks one of these numbers, and the number has already been assigned, the state should search its Database to see if it can locate the unique number in question. If not, the voter should be permitted to volunteer other identifying information such as home address, driver's license number or SSN. An application should only be rejected if the state has substantial affirmative evidence of ineligibility.

Issue Analysis:

Why Voters Should be Identified by a Unique Number

Identifying voters by a unique number makes it easier for states to spot and remove duplicate registrations. Since people's names, addresses and driver license numbers can change, assigning a unique identifier to a voter that can stay with that voter throughout his or her lifetime allows for more efficient maintenance of the voter registration Database. Additionally, utilizing a voter's unique identifier can protect voters against erroneous purges caused by voters with the same name.

Combining Different Identifying Numbers

States should avoid using a combination of identifying numbers, such as a hodgepodge of driver's license and social security numbers. Using numbers for voting that were assigned for a different primary purpose may undermine the point of a consistent number over time. For example, if a voter gets a new driver's license after an old license expires or the voter moves within the state, he or she may have a new driver's license number – but should still have the same number on the statewide voter registration Database, to ensure that the information isn't unnecessarily duplicated on the system.

Voter Enfranchisement

No registration information provided by a voter should be rejected on the basis that any given application isn't identified using the individual's unique number. If the unique number can be obtained through use of other state databases, it should be filled in on the voter's behalf; if not, a new number should be assigned. States should take care not to create extra barriers to voter registration and should never reject a voter registration application for failure to provide unnecessary information. Unique identifying numbers should be given to every voter.

Privacy

Using any kind of identifying number creates privacy concerns since registration lists are sold or granted by states to political parties (and various other groups). Some believe that selling lists with these identification numbers allows relatively easy access to personal information unrelated to voting. Even though the unique identifying number may not itself be protected by federal or state privacy statutes, in order to reduce privacy concerns states should remove these identifying numbers before making such lists available. This is another reason not to use an existing identifying number – like a social security number – for voting purposes. According to Federal Trade Commission, identity thieves frequently use SSNs as a key to access the financial benefits available to their victims.

Reduce Confusion

Once a voter is assigned a unique identifying number, that number should stay with the voter for the rest of the time he or she spends in that state. For example, a state should never retract a voter's identifying number and assign a new number if the voter moves to a different county in the same state. The Database works on a state-wide level and a voter's identifying number should be recognized by all counties, at least for the duration of a voter's residence in the state.

Accessing Database Information

Statutory Requirements:

- HAVA neither requires states to permit voters to gain access to their registration information, nor prevents states from permitting them to do so.

- HAVA requires that states "provide adequate technological security measures to prevent unauthorized access" to Database lists. 42 U.S.C. § 15483(a)(3)

- Any election official, including local election officials, "may obtain immediate electronic access to the information" in the Database. 42 U.S.C. § 15483 (a)(1)(A)(v)

Concerns & Solutions:

- Accuracy: Voters should have access to their own Database information so they can confirm that they are registered, verify the accuracy of their registration information, and identify and correct any errors.

- Efficiency: Allowing voters to have easy access to their Database information, including election precinct and polling place, will reduce voter confusion concerning where to vote and, therefore, reduce the need for provisional balloting.

- Security: Permitting voter access to Database information can decrease security because more users are on the system making it more accessible to hackers.

- Privacy: Permitting voter access to Database information can decrease the security of individual voters' private information.

Accessing Database Information continued

Recommendations

Voter Access:

- **Best Practice:** States provide both online and telephonic access to information contained in the Database (including a voter's polling place) for purposes of verifying the accuracy and completeness of their registration information. This information is available only once information unique to any given voter is entered. States permit voters to obtain directions from their home address to the proper polling place and, where appropriate, to view a map of those two locations without requiring any log-in information.

- **Avoid Where Possible:** States allow voters only online access to information contained in the Database for the purposes of verifying the accuracy and completeness of their registration information, with no instructions on how to correct inaccurate information.

- **Never:** States do not allow any public access to information contained in the Database.

Election Official Access:

- **Best Practice:** Access to the Database is governed by a login code; multiple levels of login code establish different tiers of access to Database information.

- **Never:** Election official access to more private Database without password protection.

Issue Analysis

Public Access

Allowing voters to access their voter registration information promotes accuracy and efficiency by allowing voters to confirm that they are properly registered and to verify the accuracy of their Database information. This allows voters an easy method by which to confirm that their registration information has been properly entered into the Database system by appropriate election officials, and supplies information on how voters can correct inaccurate information. States should provide mechanisms for voters to access and verify their information both online and over the telephone, without allowing direct access to the Database itself that could compromise Database security. Allowing voters to access and verify their registration information in this manner also promotes efficiency by preventing voter confusion stemming from erroneous registration information on Election Day and, therefore, reducing the need for provisional voting. This will help alleviate the burden on poll workers on Election Day, as well as the financial burden on states associated with provisional voting.

Polling Place Information

States should also allow voters to receive directions to their polling place from their home address. Access to polling place information online should include a map, including both the voter's address and polling place, as well as directions that direct the voter to the proper polling location, and information about polling place hours and procedures. By reducing voter confusion associated with polling place location, this practice will promote efficiency and accuracy and, therefore, reduce the frequency of provisional voting. States should not require log-in information to obtain polling place address and directions since this information does not create privacy concerns.

Security and Privacy Concerns

Giving voters access to their information, either online or by telephone, raises both security and privacy concerns. Allowing such public access increases the vulnerability of the Database to hackers and the risk of fraudulent interference by other third parties. Public access also decreases the security of private information contained in the Database because more users destabilize the system. In implementing the Database, states should ensure that appropriate security measures are implemented to protect the integrity of the Database itself and the information therein, including providing the public access to copies of information contained in the Database without providing access to the Database itself. Moreover, states should ensure that voters (or their authorized agents) have access only to their own registration information. Registration information should be accessible only after information uniquely identifying the voter is entered, either online or over the telephone. This will ensure that registration information is kept both private and secure.

Access by Election Officials

States should also take measures to ensure that the Database is directly accessed only by election officials, and only by those election officials that are properly authorized for the task at hand. To prevent unauthorized access, USER IDs and passwords should be issued to all appropriate election officials and states should prohibit access to the Database without such login information. Further, states should consider developing at least three levels of election official access: (1) access to a read-only version of the Database list (which may mask certain confidential voter information), (2) access to add individual new voter registration information and to update the information contained in each such listing, and (3) access to purge or modify the information of multiple voters on the list. Such security measures will help to ensure that the integrity of Database data is protected against possible fraud or manipulation and will facilitate keeping an audit trail of all election official interaction with the Database.

Accessing Database Information continued

Model State Practices:

- North Carolina voters can obtain polling place maps, driving directions from their homes to their polling places, and polling place images, as well as a list of all voting districts.

- South Carolina voters can check the status of absentee and provisional ballots, in addition to checking their registration status.

- Michigan's unique Publius systems allows voters to check registration status, polling place location, voting equipment for that polling place, candidate listings for the next relevant election, and all publicly available campaign contributions for those candidates. Publius also allows voters to obtain contact information for local election officials if registration information appears inaccurate. Finally, voters can use Publius to download request forms for absentee ballots.

Purging and Restoring Voters

Statutory Requirements:

- HAVA requires states to provide "[s]afeguards to ensure that eligible voters are not removed in error from the official list of eligible voters." 42 U.S.C. § 15483(a)(4)(B).

- HAVA requires states to ensure that "only voters who are not registered or who are not eligible to vote are removed from the computerized list." 42 U.S.C. § 15483(a)(2)(B)(ii).

- HAVA requires that all voters be removed from the Database in accordance with – at a minimum – the procedures established by the NVRA. 42 U.S.C. § 15483(a)(2)(A)(i).

Concerns & Solutions:

- **Transparency:** States should promulgate clear and uniform standards to govern purging.

- **Efficiency:** Voter purges should be conducted in a manner that allows voters to be efficiently restored to the voting rolls.

- **Fraud:** Safeguards must be put in place to protect voters from fraudulent purges by government officials or unauthorized users for personal or political motives.

- **Administrative Error:** Safeguards must be put in place to protect voters from erroneous purging due to human error.

Recommendations

Matching:

- **Best Practice:** States have uniform, non-discriminatory and transparent standards for determining when a "match" exists and a voter can be removed from the list. No voter is removed without a complete match of all available (and relevant) information.

- **Never:** Purging based on an exact match of information that may not be unique or purging based on incomplete matches.

Control and Oversight:

- **Best Practice:** Dispersed control over purging, with the authorization of at least two election officials required before action is allowed. All potential purges are double-checked before completion and archived on the Database to allow audit, oversight and easy restoration.

Purging and Restoring Voters continued

- **Never:** States give all control over purging to one election official without mechanisms for double-checking and oversight.

Notice:

- **Best Practice:** States require that notice of a potential purge be sent to each affected voter by both first-class mail, as required by the NVRA, and by telephone, before any purge occurs. Notice of purge also includes the opportunity for a voter to correct erroneous or omitted information and states implement safeguards to permit an improperly purged individual who actually arrives at the polls to vote.
- **Avoid Where Possible:** States give notice of potential purge to voters by first-class mail.
- **Never:** No form of notice to voters before being purged.

Additionally:

- All organized purges should be conducted no less than ninety (90) days before a primary or general election.

Issue Analysis

Standards for Removal

HAVA requires states to ensure that only those voters who are ineligible or not properly registered to vote are removed from the Database. Moreover, HAVA requires that all states establish safeguards to ensure that eligible voters are not removed in error from the Database. To that end, states should ensure that purging of a voter only occurs once an election official has confirmed that there is a complete match between all available (and relevant) information about the voter and the information contained within a registrant's listing on the Database. To satisfy the complete match standards, election officials must demonstrate an exact match with respect to at least the following fields: first name, last name, date of birth, and unique identifying number. If a unique identifying number is not available, election officials should also be required to demonstrate matches of other information guaranteed to ensure that the voter is uniquely identified, such as address and additional name information (e.g. middle name, maiden name, and name suffix.)

Control over Purging

HAVA mandates some degree of centralization of voter registration and purging by requiring that the chief statewide election official have ultimate control over the Database. Centralizing all purging activities within that office, however, could leave the Database vulnerable to par-

tisan manipulation especially if that office is held by a partisan elected official. At the same time, placing control of purging solely in the hands of local election officials could lead to disparate treatment of voters within a state. States are encouraged to protect against both of these concerns when developing clear and uniform standards to govern purging, as required by the text of HAVA. One possible solution would be to require both an official from the chief election official's office and an appropriate local election official to approve all purges, pursuant to clear, fair and published statewide purging standards. States are encouraged to develop purging standards that fit with their own administrative structure, while still providing adequate voter protection against fraud and administrative error. In any event, no purge should be effectuated without the approval of two or more election officials at different levels of government.

Oversight

In addition to developing clear and uniform standards to govern purging, states should also design the Database in a way that allows for adequate oversight with respect to purging. For example, voter purges – like all Database transactions – should be saved and separately archived to allow oversight of election official actions. The archived record should include the date and time of any purge, the identity of the user who removed a voter, the identity of the person who authorized the transaction, and the reason any record was removed from the list. Once a purge has been documented and archived, it can be independently audited to ensure that uniform purging standards have been followed, further protecting voters from the risk of fraud and administrative error. The archived purged records should be escrowed, in addition to the code for the Database and the data contained within.

Notice

HAVA also requires that the removal of any name from the Database be done – at a minimum – in accordance with the protections of the National Voter Registration Act ("NVRA"). The NVRA requires that, before removing from the Database the names of most ineligible voters, such as those whom election officials believe have moved outside of the election district, states must notify the voter and provide an opportunity to correct or explain his or her continuing eligibility.

Purging and Restoring Voters continued

Timing

As required by the NVRA, organized computer list maintenance activities and purges must be completed no later than ninety (90) days before a primary or general election. Exceptions to this rule should only be allowed for purges based on changes in the individual's eligibility within the 90-day window, such as deaths or, where applicable, felony convictions in the weeks before an election, or based on removal requests initiated by confirmed requests from the voters themselves.

Restoration of Voters

When a voter is purged, the voter should not be deleted entirely from the Database. Instead, the voter's information should be flagged as inactive or ineligible. This information should be kept securely for a set period of time rather than destroyed or deleted from the Database. Keeping purged voters' information flagged as inactive or ineligible will facilitate the efficient restoration of voters to the Database system, if and when restoration is appropriate, and will reduce confusion by allowing a given purged and restored voter to maintain the same unique identifying number. For example, when a person rendered ineligible by a felony conviction is later eligible to vote, he or she can be expeditiously restored to eligible voting status once past address information is either confirmed or updated. Similarly, a voter who was purged based on voting inactivity (and failure to respond to notice, as required by the NVRA) can quickly and easily be restored to the Database once the voter regains active and eligible status.

Model State Practices:

- Georgia requires pre-removal notification before any voter is removed from the registration list, including any voter being removed due to conviction of a felony. After notification, a voter has 14 days to dispute that he or she is removable.

- Louisiana moves purged voters to a suspended file that includes the date of voter suspension, the reason for suspension, and an indication that the voter was notified of such action. Files are kept in a separate database of suspended voters for a period of two years. This allows voters to be more efficiently restored to the registration rolls.

Failure and Recovery of Data

Statutory Requirements:

- The State election board shall include "provisions to ensure that voter registration records in the State are accurate and are updated regularly." 42 U.S.C. § 15483 (a)(4).

- "The appropriate State or local official shall provide adequate technological security measures to prevent the unauthorized access to the computerized list established under this section." 42 U.S.C. § 15483(a)(3).

- HAVA requires that each Database be "defined, maintained, and administered" by the state. 42 U.S.C. § 15483(a)(1).

Concerns and Solutions:

- **Protection:** Maintaining voter information on any kind of database puts that information at risk if the system crashes. Creating an electronic database that is capable of both preventing system failure and recovering data if the system does crash protects against the loss of vital voter information.

- **Security:** Even when the Database is functioning properly, data can still be lost either by mistake or fraud. Creating ways of recovering lost data provides for a way to redress these problems.

Recommendations

Securing the Software:
- All software (including both object and source code) for building, operating and maintaining the Database should be placed in escrow periodically.

Securing the Data:
- **Best Practice:** The Database is implemented as two replicated, fully mirrored systems, with each system's copy of the data synchronized continuously and in real-time.

- **Avoid Where Possible:** The Database is backed up once a week, and such weekly backup copies are preserved for several election cycles. Every 24 hours a back up copy of all changes to any Database data is also backed up.

Failure and Recovery of Data continued

- **Never:** Failing to establish any standards for creating back-up copies of the data or a process for restoring the data in the event of system failure or data corruption.

Encryption:

- All the data stored on the Database must be encrypted. All transmissions of that data, and any backup or archival tapes of the software or data relating to the Database must also be encrypted.

Trained Employees:

- **Best Practice:** States require that specific employees be trained and certified to manage and address technological problems with the Database. For small-scale problems, these employees should be dispatched throughout the state. States also require that any large problem be immediately addressed and that the employee fixing the Database be monitored.

- **Never:** No one within the state is trained to handle technological Database issues.

Maintenance

- Establish a schedule of software/hardware updates and general maintenance and require that these are performed only when authorized and overseen by an election official.

Ownership

- The state should maintain ownership of license rights in all customized software, and should own all data in the Database.

Issue Analysis

Use of Escrow for the Code

Because the data contained in the Database could be tampered with through manipulation of the source code, the code should not be made public. Allowing only the state to access the code, however, opens election officials up to allegations of fraud. Putting the code in escrow would allow the code to be protected – and would at the same time preserve a clean copy should the Database experience any major failures. Placing the code in escrow will also allow independent auditing of the source code to occur, when appropriate. Both the object and source code for the Database should be escrowed, as well as the object code for any other programs, tools or utilities required in order to operate the Database. Escrowed tapes should be encrypted to minimize risk of disclosure from inadvertent or intentional acts. The escrow should be in a secure and protected location.

Saving the Data

Because a Database may experience occasional failure, a copy must be saved on a separate system in order to prevent its loss. While it may be costly to replicate the Database completely, that cost will

usually be less than the cost of rebuilding the Database in the event of catastrophic failure. In addition, the Database can and should be designed so that all the changes to the data are saved every 24 hours – and that these discrete changes, as well as the full backups, are escrowed for several election cycles. Together, these measures will ensure that all pertinent data can be recovered if the Database fails. Any copies of data from the Database should be saved in a secure and protected location.

System Continuity

For system continuity the ideal is to implement the Database as two separate, fully mirrored, real-time synchronized systems so that if the primary Database suffers a system failure or degradation, the secondary system will immediately step-in with data as up-to-date as on the primary system. The users may never even know that there was a system problem. While it is certainly compelling to do this during an election cycle, it may be cost prohibitive to do this the rest of the time. An alternative during these non-election cycles is to have a second set of equipment loaded with recent copies of the software and data that can be turned on and operating within hours of a failure of the primary system. The amount of work necessary to keep the data on the secondary system current will be determined by how often the primary system's data is backed up to the secondary system. To recover from natural disasters or power outages, the secondary system should be located in a different location, even in a different city, than the primary system. Note that the secondary system should not serve double duty as the escrow. The escrow serves a different purpose and should also be kept in a different location; it does not typically include equipment, but just copies of the code and data for the Database.

Encryption

States should require that data on the Database be encrypted. With encryption, the data stored on the Database is much less valuable to someone who accidentally or purposefully gains access to it. This will ensure that the information is secure and that it won't be tampered with. Moreover, because some voter information is personal, data encryption will ameliorate fears of identity theft. Similarly, electronic interfaces between the Database and other state databases and systems, such as the DMV, should be encrypted. Moreover, all backup copies of the data stored on the Database should be encrypted, including those sent to escrow.

Training

Equally important for securing the data is ensuring that the election officials who work with it are adequately trained and supervised. Because officials who are responsible for addressing Database failures are capable of interfering with the stored data, there should only be a few qualified officials who are entrusted with the job. Similarly, when software and hardware have to be updated, officials working with the Database must be supervised.

Notes:

Notes: