

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA

FLORIDA STATE CONFERENCE OF THE
NATIONAL ASSOCIATION FOR THE
ADVANCEMENT OF COLORED PEOPLE
(NAACP), as an organization and
representative of its members; *et al.*,

Plaintiffs,

Vs.

KURT S. BROWNING, in his official
capacity as Secretary of State for the State of
Florida,

Defendant.

Civil No. 4:07cv402 spm/wcs

**DECLARATION OF
ANDREW BORTHWICK
IN SUPPORT OF
PLAINTIFFS' MOTION FOR A
PRELIMINARY INJUNCTION**

Pursuant to 28 U.S.C. § 1746, I, Andrew Borthwick, hereby declare as follows:

1. I am Principal Scientist at Spock Networks, Inc. ("Spock"), a company specializing in the indexing and classifying of public information about people from diverse sources. Our work depends on identifying, selecting, and matching discrete information about individuals from publicly available databases and websites. My current office is located at 1450 Veterans Boulevard, Redwood City, California 94063.

2. I am also a member of the Board of Directors, and former President and Chief Executive Officer, of ChoiceMaker Technologies, Inc. ("ChoiceMaker"), a company that I co-founded in 1998. ChoiceMaker is a data quality company specializing in the design and development of record-matching software. I submit this declaration in support of Plaintiffs' Motion for a Preliminary Injunction.

CLERK
U.S. DISTRICT CT.
NORTHERN DIST. FLA.
TALLAHASSEE, FLA.

2007 SEP 17 PM 2:59

KRB
RECEIVED

Background

3. I earned a B.A. from Oberlin College in 1988, graduating Phi Beta Kappa. I earned an M.S. and Ph.D. in Computer Science from New York University. My Ph.D. was awarded in 1999. My doctoral dissertation discussed a maximum entropy approach to named entity recognition, which in broad terms involves a learning technology that builds a model of the human decision-making process for identifying and categorizing proper names, in order to find names in context in newspaper text. For example, my dissertation discussed an approach useful for distinguishing articles about Calvin Klein, the individual, from articles about Calvin Klein, the company. I co-founded ChoiceMaker to apply the technology discussed in my dissertation to the record-matching field.

4. My academic expertise is in the fields of record-matching, machine learning, and computational linguistics. Of greatest relevance here is my background in the first, "record matching," which is a common term of art in the field of information science (also referred to as "informatics"). Record-matching refers to the process of identifying entries in a database (known as "records") that pertain to the same entity or person represented in other records, either in the same database or in another database. Often, these records are matched by comparing particular categories of data (known as "fields") within each record, such as a person's first name, last name, and date of birth. The science and challenge of record-matching involves identifying matching entries in the face of errors in one or both sets of data, or of inconsistencies between the data. I was

awarded U.S. Patent No. 6,523,019 in 2003 for a machine learning approach to record-matching, and U.S. Patent No. 7,152,060 in 2006 for a method of decreasing the processing time required for accurate record-matching through more efficient searching. I also am the co-inventor of one other process concerning record-matching with patent applications pending before the U.S. Patent and Trademark Office.

5. In 1998, I founded ChoiceMaker, and I was joined as co-founder by my business partner, Arthur Goldberg. ChoiceMaker is a data quality company specializing in record-matching software. Among other functions, ChoiceMaker software allows entities to identify corresponding records within and between databases. From 2000 to 2005, ChoiceMaker won a prestigious series of Small Business Innovation Research grants from the National Science Foundation for its research into a maximum entropy approach to approximate record matching.

6. In 2005, ChoiceMaker was awarded a contract with the U.S. Centers for Disease Control ("CDC") to use our record-matching system for the National Electronic Disease Surveillance System. This CDC surveillance project tracks the emergence and incidence of diseases in all 50 states in order to facilitate reporting to the CDC and to identify outbreaks of infectious diseases. The ChoiceMaker system was also purchased by nine states to track the academic records of every student in K through 12 public education, to support implementation of the No Child Left Behind Act. ChoiceMaker has also won multiple contracts with the New York City Department of Health to track immunizations of children, lead tests, and the incidence of communicable

diseases – which requires matching records from laboratories, hospitals, and clinics, in the face of numerous errors. ChoiceMaker was also used for the World Trade Center Health Registry to compile a register of everyone near the World Trade Center on 9/11 in order to track long-term health issues. ChoiceMaker was also awarded a contract with the New South Wales, Australia, Department of Health to develop a system for epidemiological research.¹

7. In 2007, I became Principal Scientist at Spock Networks, Inc., which was founded in or around early 2006. Spock Networks is the premier online leader in personal search technologies, helping users find and discover people. Its success depends on its ability to accurately gather information on individuals, and sophisticated record linkage techniques are essential to this goal. That is, the principal Spock Networks product rapidly, reliably, and accurately finds public information that “matches” a specific individual while excluding information from individuals who appear very similar but are not in fact the same person.

8. I have published on, among other things, techniques involved in record-matching, including articles for peer-reviewed conferences in 1999 and 2004. A complete list of my publications is included in my *curriculum vitae*, a copy of which is attached as Exhibit A. I was invited to speak on record-matching at the First Workshop on Data Cleaning, Record Linkage, and Object Consolidation, in conjunction with the

¹ ChoiceMaker has never been, and is not now, affiliated with ChoicePoint, Inc., Database Technologies (DBT Online), or any of their successors in interest.

Association for Computing Machinery Special Interest Group on Knowledge Discovery and Data Mining's Ninth International Conference on Knowledge Discovery and Data Mining, in Washington, D.C., on July 17, 2003. In addition, I have given presentations at the Massachusetts Institute of Technology's annual International Conference on Information Quality, the annual Information Quality Conference, and the annual National Immunization Conference, among others.

9. I regularly review publications in the record-matching field, in order to ensure that I am well versed in the current state of the art. Representative publications of this sort include *Institute of Electrical and Electronics Engineers ("IEEE") Transactions on Pattern Analysis and Machine Intelligence* and *IEEE Transactions on Knowledge and Data Engineering*. I am a member of the IEEE, the world's leading professional association for the advancement of technology, and the Association for Computing Machinery, an international scientific and educational organization dedicated to advancing the arts, sciences, and applications of information technology. I have submitted an expert declaration before a court in only one other matter, a case in Washington State that also pertained to the fallibility of record-matching processes in the voter registration context. My billing rate for this matter is \$150 per hour.

Summary of Conclusions

10. For this case, I was asked to examine whether record-matching protocols used in Florida's voter registration program will result in a significant number of errors. In particular, I was asked to explain whether and why, in my professional opinion, errors endemic to information gathering, entry and maintenance, along with immaterial differences and inconsistencies across different databases, will result in the failure to match information from two different sources pertaining to the same individual. In the technical language of my field, the question I explored was whether an exact comparison of the characters in multiple fields of two different records, each filled out (or "populated") at different times by manual data entry from different handwritten forms or from information given orally to a data entry clerk, would likely result in substantial numbers of "false negatives" – that is, registration records for which the name and identifying information do not "match" the name and information in another database when, in fact, both records reflect the same person. For example, a "false negative" will result when a woman registers to vote with her married name, her maiden name is listed on her Social Security record, and the two records fail to "match."

11. To prepare to give my opinions in this case, I read the applicable federal and State laws and regulations, including relevant portions of the Help America Vote Act (and in particular 42 U.S.C. § 15483) and Fla. Stat. § 97.053(6), my own academic and professional work, and relevant publications in the field. Those publications include papers in the *Statistical Research Report* series of the U.S. Bureau of

the Census, articles published in peer reviewed journals such as *Computers and Biomedical Research* (now known as the *Journal of Biomedical Informatics*) and the *Journal of the American Medical Informatics Association* (AMIA), and proceedings of the AMIA's annual symposium. I also reviewed documents provided to the Plaintiffs, including letters from the Florida Secretary of State to the Advancement Project and others, describing the registration process in Florida.

12. To learn more specifically about Florida's record-matching process, I also reviewed documents including the "*Social Security Verification*" System Specification distributed by the American Association of Motor Vehicle Administrators in August 2004. In particular, I reviewed the Help America Vote Verification ("HAVV") process (also referred to as a "transaction") and the matching protocol described on pages 26 and 27 of that document; a copy of the relevant pages is attached as Exhibit B. I also reviewed the Guide to the Florida Voter Registration System ("FVRS") dated September 7, 2005, and the registration protocol described on pages 41-46 of that document; a copy of the relevant pages is attached as Exhibit C. I also reviewed the public presentations of Peter Monaghan, the Social Security Administration's Senior Advisor to the Office of Programs, dated February 6, 2006, and February 12, 2007, relating to audits that the Social Security Administration has performed relating to its matching of voter registration information. Copies are attached as Exhibits D and E. I reviewed similar reports of audits of the voter registration information matching process by election officials in New York City. A copy is attached as Exhibit F.

13. Based on my academic and professional experience with record matching, and additional research and analysis I performed, including my review of relevant materials from Washington State, and based on my understanding of Florida's matching protocols, I conclude that the voter registration matching processes used for Florida voters will result in a significant number of "false negatives": records that pertain to the same individual but which are unable to be matched. If Florida effectively conditions registration on a successful "match," a significant number of valid voter registration applications will be rejected as a result. These errors are likely to occur even if the applicants do not make any mistakes or provide any incorrect information on their registration forms. It also is my opinion, based on studies of similar protocols, that the rate of such "false negative" errors will be substantial, and could reach as high as 30% overall. Indeed, the Social Security Administration has reported that its attempts to match voter registration records to its own records have thus far failed 46.2% of the time.

The Process of Record Matching in Florida

14. I understand that in 2006, the Secretary of State of Florida, in conjunction with other State and federal agencies, began to attempt to match certain information provided on new voter registration forms with information stored on other databases. Based on documents that I have reviewed pertaining to Florida's voter registration process, I outline in broad terms below my understanding of the process of record matching as it is performed in Florida.

15. *First*, I understand that citizens fill out a voter registration form by hand with their identifying information. That information includes: name, date of birth, and either a driver's license number (or non-driver's ID card number) or the last four digits of their Social Security number (if the applicant has such a number). A true and correct copy of Florida's registration form available online from the website of Florida's Secretary of State is attached hereto as Exhibit G. Registrants may also supply their identifying information orally to a data entry clerk. The completed forms are then submitted to State or county officials.

16. *Second*, I understand that data entry operators working for the State or county will input the data contained on the voter registration forms into one or more databases that serve as temporary, electronic storage for such new registration records.

17. *Third*, I understand that each new electronic registration record will be submitted to State officials, who will cause certain pieces of information in the registration record to be compared automatically either to the Social Security Administration database or to the State Department of Highway Safety and Motor Vehicles ("HSMV") database. This is done in an attempt to "match" the information contained in the voter registration record to the information contained in the database. For matching with the Social Security Administration database, my understanding is that Florida is using a protocol in which each character of the first name, each character of the last name, each character of the year of birth, each character of the month of birth, and

each character of the last four digits of the applicant's Social Security number, as entered in the voter registration record, must match exactly with the corresponding character or the corresponding field of the Social Security Administration database. For matching with the HSMV database, my understanding is that Florida is using a protocol in which at least the driver's license or non-driver's identification card number and the first four letters of the first name and last name must match exactly with the characters of the corresponding field in the HSMV database.

18. *Fourth*, I understand that if the State finds a "match," the person who filled out the form, if otherwise eligible, will be registered to vote. If the State does not find a "match," the person who filled out the application will not at that point be registered to vote, although I understand that in certain circumstances, there may be some further review, and that elections officials will attempt to correspond with such applicants to try to resolve the problem.

19. Based on this information, it is my opinion that record matching as I understand it will be conducted in Florida will likely result in high numbers of false negatives. That is, I am confident that attempts to match information in new voter registration records to information in other State and federal databases will fail for reasons unrelated to the accuracy of information provided by the applicants or the eligibility of applicants to vote.

Common Errors Related to Record Matching

20. There are several reasons why large databases are prone to errors that make the process of record matching imperfect. The point is a rather basic one, but it has profound consequences when attempting to match individual records in one large database with records in another database: typos, misplaced information, incorrectly transcribed data, and immaterial spelling and punctuation differences in either one or both of the databases may result in two records for the same person not “matching.”

21. **Data Submission.** Errors within individual records of large databases may be caused by mistakes in data submission. I am not referring to false information, but mistakes in the form in which the data is submitted. Such mistakes can include minor errors made by individuals filling out forms, such as writing information in one place when the information should be written in another. These immaterial mistakes may appear in the registration record or in the government database being matched – or in both. For example, a person may write her day of birth in a space reserved for the month of birth. If this were to occur in Florida, that person’s birth date as entered from her registration form will not match the birth date as recorded on the database with which the State will compare her identifying information.

22. **Data Entry.** Errors within individual records of large databases may also be caused by mistakes in the process of entering the data in the computer. Such errors may occur when an operator strikes an incorrect key, incorrectly hears information

given orally, or incorrectly reads information from a form. For example, a data entry operator may type an "a" when an "o" is written, or type a "d" when a "c" and an "l" are written together. Common data entry errors also include:

- omitting characters (e.g., "JOHN" becomes "JON");
- adding characters (e.g., "OWEN" becomes "OWENS");
- transposing characters (e.g., "SIERRA" becomes "SEIRRA,");
- substituting characters (e.g., "THOMAS" becomes "THOMAS"); or
- any combination of the above.

23. Other data entry errors may occur when an operator enters information in the wrong field (e.g., inverts day and month in fields provided for the date of birth). Operators also separate compound last names into the "middle name" and "last name" fields or, conversely, combine a middle and last name into a single last name (e.g., "GABRIEL" "GARCÍA" "MÁRQUEZ" becomes "GABRIEL" "GARCÍA MÁRQUEZ"). Such errors include:

- omitting fields (e.g., "MARIE MAUDE" becomes "MARIE");
- adding fields (e.g., "JAMES THOMAS" becomes "JAMES J THOMAS" or "MR JAMES THOMAS" or "CAPT JAMES THOMAS");
- transposing fields (e.g., "JAMES THOMAS" becomes "THOMAS JAMES", or "LU BAO" becomes "BAO LU");
- substituting fields (e.g., "JIMMY THOMAS" becomes "JAMES THOMAS");
- improperly separating fields (e.g., "JEAN-CLAUDE" becomes "JEAN" "CLAUDE");

- improperly combining fields (e.g., “DEBBIE” “WASSERMAN” “SCHULZ” becomes “DEBBIE” “WASSERMAN-SCHULZ”); or
- any combination of the above.

24. I am a member of the Association for Computing Machinery, and I have reviewed relevant portions of the ACM’s February 2006 study *Statewide Databases of Registered Voters*, a copy of which is attached as Exhibit H. This study recognizes both that “[m]ost errors in individual database records occur during data entry,” and that “[w]hile quality control systems and appropriate supervision of data entry may reduce data entry errors, some errors will inevitably occur. . . . Changes that are primarily entered in other state databases – such as changes in marital status and court approved name changes – also compound the challenge to accuracy.” Exh. H at 21.

25. In my extensive experience working with databases containing similar kinds of personal information, the errors described in paragraphs 22 and 23 can be quite common. One reliable study found that the names of 23-37% of the patients in several medical databases were misspelled in at least one database record; a copy of this study is attached as Exhibit I. Another study reported that approximately 26% of records in a Florida social service database included city names with apparent misspellings, including more than 40 different spellings of “Fort Lauderdale”; the study’s relevant pages are attached as Exhibit J.

26. If any one or more of the errors described in paragraphs 22 and 23 were to occur in Florida in the registration record itself and/or in the database with which

the record will be matched, the name as entered from the individual's registration record will not exactly match the name as recorded in the database with which the State will compare the individual's registration information.

27. Data entry operators commonly commit errors when they input names, but they also commit many of the same types of errors when they input numbers. Such errors are specifically acknowledged to occur with respect to Social Security Numbers. The leading expert on record matching for the U.S. Bureau of the Census estimates that in one large California employment database, given these types of errors "[o]ver a period of twenty years, the records [associated] with each individual can expect to contain *at least two errors* where the [Social Security Number] has been mis-keyed or transcribed improperly" (emphasis added). A copy of this publication is attached as Exhibit K.

28. **Data Maintenance, Storage, Transfer, and Transformation.**

Once a record is created for an individual applicant, the State must maintain, store, transfer and, often, transform the data contained in that record. Federal and State officials must perform similar tasks with respect to data contained in the Social Security Administration and HSMV databases. These processes are also prone to error, for example, when computer viruses cause file corruption; when the data input locally, in Florida's 67 county election management systems, is transferred to the State; and when database fields are added, modified or deleted and, accordingly, data is split, changed, or

consolidated. In my experience, such transfers can lead to unintended changes in the underlying data.

29. The ACM's study, *Statewide Databases of Registered Voters*, also recognizes that glitches can create problems in large databases. As the study states:

Databases also can be inaccurate or unreliable because of computer viruses, programming errors, and system failures. For example, in 2003 the Maryland Motor Vehicle Administration (MVA) offices were attacked by a computer worm. The worm shut down the MVA's computers and telecommunication systems, cutting them off from all forms of remote communication and disrupting operations in all 23 MVA offices located throughout the state. A second event occurred on January 20, 2004, when the MVA could not process work on the mainframe computer for about an hour after opening. The problem was characterized as a computer glitch.

Exh. H at 24.

30. There is no single standard industry algorithm or process for maintaining, storing, or transforming data; different entities use different processes for these purposes. As noted on page 14 of the "*Social Security Verification*" *System Specification*, for example, there will be "many different types of computers on the [AAMVA] network, each possibly having a different data-encoding scheme." Different entities using different conventions, or transferring data using different encoding systems may, because of incompatibilities, cause modifications in the data they maintain that will lead to unmatched information.

31. If any of these modifications were to occur in Florida, affecting the registration record itself and/or the database the record will be matched with, the information as entered from the individual's registration record will not exactly match the information as recorded in the database with which the State will compare her identifying information.

32. **System Errors.** Online computer systems intermittently experience system errors or other "down time." The Social Security Administration is not immune to these errors; the "*Social Security Verification*" *System Specification* describes "program problems, network interface errors, database errors, program aborts, [and] the more common system error[,] when the SSA file is off-line." Exh. B at 17.

33. If such system errors occur when a Florida registration record is submitted, at least during the error period, the information on that record will not be able to be matched with information in the offline database.

34. **Natural Data Inconsistency.** In addition to the errors described above, the process of matching information in different records itself produces false negatives because of superficial discrepancies between those records that do not reflect inaccurate information. For example, names are not truly standardized, nor are they fixed. People adopt nicknames, use shortened names, pick up or drop middle names, take their spouse's names, and/or change the spelling of their transliterated names – and they do so even in formal government documents. In addition, different applicants or different data entry operators (and even the same people on different occasions) may transliterate

non-English characters in different ways. Thus, two records for the same person may show different names, like a maiden name or married name. Similarly, data entry operators often use default assumptions to fill in missing information (*e.g.*, choosing the first of the month when no day of the month is given).

35. Common examples of natural data inconsistencies that may cause false negatives include:

- nicknames (*e.g.*, “ELIZABETH” versus “LIZ”);
- maiden names (*e.g.*, “REBECCA JONES” versus “REBECCA SMITH”);
- husband’s names (*e.g.*, “MRS. JOHN SMITH” versus “MRS. REBECCA SMITH”);
- punctuation (*e.g.*, “O’BRIEN” versus “O BRIEN” or “OBRIEN”)
- compound last names (*e.g.*, “GABRIEL” “GARCÍA MÁRQUEZ” versus “GABRIEL” “GARCÍA” “MÁRQUEZ”);
- first or middle initials (*e.g.*, “F. SCOTT FITZGERALD” versus “FRANCIS S. FITZGERALD”);
- name change due to religious conversion (*e.g.*, “MUHAMMAD ALI” versus “CASSIUS CLAY”); or
- any combination of the above.

36. Similar data inconsistencies arise when confronting names common within certain ethnic communities:

- immigrants adopting “Americanized” names, for all purposes or just some purposes (*e.g.*, “GRACE KIM” versus “HYUN KIM”);
- name change due to different status in the community (*e.g.*, in Burmese, “MAUNG TIN” (for younger men) versus “U TIN” (for married men));

- mistaking a title for a first name (e.g., “MAUNG TIN” versus “TIN”);
- transliterated names or diacriticals (e.g., “MUHAMMAD” with “MOHAMMED,” or “SCHRÖDER” with “SCHRODER” or “SCHROEDER”);
- alternative spellings (e.g., “DE LA CRUZ” with “DELACRUZ”); or
- any combination of the above.

37. In my extensive experience working with databases containing similar kinds of personal information, the discrepancies described in paragraphs 35 and 36 can be quite common. If any of the natural discrepancies described in paragraphs 35 and 36 were to occur in Florida, creating immaterial differences between the registration record itself and the database the record will be matched with, the information as entered from the individual’s registration record will not exactly match the information as recorded on the database with which the State will compare her identifying information.

38. My wife’s name provides an example of how such trivial differences can cause record-matching problems. My wife usually represents herself as “Sarah C. Borthwick,” and signs personal checks that way. But she is registered to vote in New York as “Sarah E. Caguiat Borthwick.” Her New York driver’s license shows her name as “Caguiat-Borthwick, S”. And she appears in Social Security Administration records as “Sarah E. Caguiat.” If she attempted to register to vote in Florida as “Sarah Borthwick,” the information in her application would likely not match information in either the driver’s license or Social Security databases.

Errors Common in Particular Communities

39. Certain errors contributing to difficulties in record-matching are more prevalent among particular racial and ethnic communities. For example, in Hispanic or Latino communities, it is common to use either maternal or paternal last names, or both. These names are often supplied inconsistently by the individual or entered inconsistently by the data entry operator such that the “middle name” and “last name” fields in the resulting record are inverted, separated, or combined. For example, “José Luis Rodríguez Zapatero” might have “Zapatero,” “Rodríguez,” or “Rodríguez Zapatero” entered as his last name.

40. In African-American communities, names derived through modification of more traditional spellings are more common than in other racial or ethnic communities. These names are more likely to be misspelled in data entry. For example, one study reports that “Jazmine,” “Jasmin,” and “Jazmin” are all girls’ names much more common among African-Americans. A copy of this study is attached as Exhibit L. These names may all be misspelled as “Jasmine” in data entry, thus creating errors when an exact character-by-character match protocol is applied. Moreover, names that are unique to a particular individual are also more common in African-American communities. The same study cited above, for example, found that African Americans in California are six times more likely to have a unique name than are Caucasians. These names may be unfamiliar to data entry personnel (of any race or ethnicity), and are more likely to be misspelled in a database.

41. Transposition of the “first” name and “last” name is more common with regard to individuals of Chinese descent, many of whom present their family name first and their given name second, contrary to the usual American practice. A data entry operator might not know which name in “Lu Bao” is the first name and which is the second, and enter it based on any variety of conventions, such as assuming that the first name listed is the given name. If Mr. Lu’s name is transposed in one record, that name will not match exactly to the other record. In my experience, individuals of Chinese descent also frequently adopt names considered to be common “Western names,” but use these “Western names” inconsistently in official records. The following example illustrates both phenomena: a Chinese woman named “Wang Fei” might inconsistently put her first name before her last name (*i.e.*, “Fei Wang”); use a Western form of her first name (*e.g.*, “Faye Wang”) or a Western name not derived from her first name (*e.g.*, “Grace Wang”); and/or use a Western form for both her first and last names (*e.g.*, “Faye Wong”).

42. In communities that do not use the Roman alphabet in their primary language, such as East Asian, Middle Eastern, Hellenic, and Slavic communities – or communities using diacritical marks not found in English, such as the umlaut or tilde – inconsistent transliterations are common. Arabic names like “Mohammed,” for example, are transcribed differently depending on the country of origin. Three variants include “Muhammad,” “Mohamed,” and “Mahomet.”

43. The transposition of the date and month of birth is more commonly found with regard to recent immigrants, who may be accustomed to presenting dates in a day-month-year convention, which is commonly used in Europe, Africa, the Middle East, and Asia. Thus, someone whose date of birth is May 6, 1980 might input her name as “6/5/1980,” and since that is a valid date under the American month-day-year convention, her record will reflect that her birth date is June 5, 1980.

44. Mismatched surnames due to a maiden name or married name are more common, of course, with regard to women. Thus, to use my wife as an example again, whether she registers to vote using a compound last name without a hyphen, a compound last name with a hyphen, or my last name, the information entered from her registration record will not exactly match the information in the Social Security Administration’s database, where she appears under her maiden name.

The Impact of Errors and Non-Standardized Data on Record Matching

45. Attempts to match records using exact, character-by-character matching – referred to in the industry as “deterministic” matching – are highly sensitive to all of the errors and discrepancies described above. The failure to match information because of such errors and discrepancies would result in false negatives – *i.e.*, the failure to match database entries that in fact belong to the same individual.

46. Data from several reliable studies show that, in similar circumstances, false negative rates generated by deterministic matching protocols can

reasonably be expected in the range of 20-30%. For example, in one reliable study, the U.S. Bureau of the Census suggested that using a deterministic match on census data would have resulted in a false negative rate of about 25%; a copy of this study is attached as Exhibit M. Another reliable health care study found a false negative rate of about 22% using a deterministic protocol. Exh. I at 503-04. And yet another reliable study found that a deterministic protocol missed 17-30% of records belonging to the same individuals; a copy is attached as Exhibit N.

47. Deterministic matching protocols have shown similar failure rates in practice. For example, through mid-June of 2006, I understand that Washington State compared information on new voter registration forms to information maintained in motor vehicle and Social Security records through a deterministic matching protocol. Through this process, no match was found for 16% of new forms statewide, and 30% of the records submitted in the state's most populous county (King County) were unable to be matched. These "no match" rates are consistent with the false negative rates in the studies above. That is, it would be consistent with these accounts to find that 30% of the forms submitted in King County failed to match information in the motor vehicles or Social Security databases, but actually represented individuals accounted for in the motor vehicles or Social Security databases.

48. As noted above, I have reviewed the *Social Security Verification System Specification* prepared by the American Association of Motor Vehicle Administrators in August 2004, and, in particular, the HAVV transaction described on

pages 26 and 27 of that document. Exh. B at 26-27. As described in that document, the HAVV transaction uses a deterministic match protocol in which a system will attempt to match the last name, first name, month of birth, year of birth, and last four digits of the Social Security number of a target record to the same elements of records in the Social Security Administration database. A successful match will be reported only when each character of each such field in the target record matches precisely each character of each corresponding field in the Social Security Administration database. Pursuant to the same document, I understand that an unsuccessful match will be coded as a "system error," "invalid input data," or "no match found"; no more specific information will be returned to the state indicating why a match could not be found, more precisely locating the source of the error.

49. The HAVV protocol is not designed to account for, and will not readily account for, the errors described above; the protocol for matching with the HSMV database is similarly susceptible to the same errors described above. Moreover, particularly but not exclusively in the HAVV protocol, the requirement that *multiple* fields exactly match compounds the error rate expected for an exact match on any individual field.

50. Page 10 of the above-noted 2006 presentation of Mr. Monaghan, the Social Security Administration's Director of Information Exchange, states that no match was found in 28.5% of 143,000 queries submitted in the period before his presentation. Exh. D at 10. Page 9 of Mr. Monaghan's 2007 presentation reports that of

the 2.6 million queries submitted by 2007, no match was found in 46.2% of the queries. Exh. E at 9.

51. Assuming that the Social Security Administration used the deterministic HAVV transaction to seek matches for voter registration records, the reported 28.5% “no match” rate described in paragraph 49 is consistent with the rate of false negatives found in other published accounts of deterministic matching. The 46.2% “no match” rate reported in 2007 is greater than the false negative rate reported in many other accounts, but given the acknowledged errors in the Social Security database, the multiple points at which error may be introduced in the process of entering voter registration data, and the HAVV protocol’s use of deterministic matches on multiple fields in combination, it is not unreasonable to believe that the 46.2% “no match” rate in fact represents false negatives. That is, it would be consistent with these accounts to find that 46.2% of the queries submitted to the Social Security Administration failed to match information in the Social Security database, but actually represent individuals accounted for in the Social Security database.

52. Moreover, in my opinion, some voters will probably not be provided an effective opportunity to resolve a “false negative.” For example, although I understand that Florida election officials may attempt to correspond with unmatched registrants, data entry errors impacting name and address will probably prevent some correspondence from reaching its intended target.

53. I have reviewed the May 15, 2003 appraisal of Virchow Krause & Company, a prominent Midwest accounting and consulting firm retained by the Wisconsin State Elections Board to evaluate project proposals for Wisconsin's statewide voter registration database. A copy of the relevant portion of this appraisal is attached as Exhibit O. I agree with the appraisal's conclusions regarding the difficulty and likely effect of matching in this context:

Name matching and validation issues are very complex (e.g., matching Margie L. Smith with Margaret Smith), and are made even more complex when aliases and name changes are considered. . . . Even a 1% error rate on an interface validating names, driver license numbers, etc. could generate tens of thousands of bad matches in an error log, well beyond any ability for the [state, county, or local] users to manually verify the errors. . . . [¶] All vendors suggested that incomplete or unmatched records be ignored, because the time to resolve, cost to resolve, and potential for error and disenfranchisement was too high.

Exh. O at 20.

54. In sum, the matching systems that I understand Florida is using, described in paragraphs 17 and 48, are prone to many errors – especially false negatives. In my opinion, such systems would generate failed matches for individuals who are, in fact, legitimately represented in the target database. When comparing two data sources of significant size – as Florida is doing here – records representing the same individual would fail to match even if the Secretary of State used protocols representing the best available technology. If matching is effectively a prerequisite to registration, the use of any match process will result in eligible voters being denied the right to vote.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, and that this Declaration was executed on September 15, 2007 in Palo Alto, California.



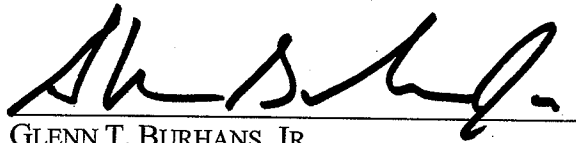
ANDREW BORTHWICK

CERTIFICATE OF SERVICE

Undersigned counsel hereby certifies that a copy of the foregoing *Declaration* was served via HAND DELIVERY this 17th of September, 2007 upon the following:

Kurt Browning, Defendant
Secretary of State
Florida Department of State
R.A. Gray Building
500 South Bronough Street
Tallahassee, FL 32399-0250

GREENBERG TRAUIG, P.A.



GLENN T. BURHANS, JR.
FLA. BAR NO. 605867
101 EAST COLLEGE AVENUE
TALLAHASSEE, FLORIDA 32301
TEL. (850) 222-6891
FAX (850) 681-0207

ANDREW BORTHWICK, Ph.D.

1453 Kings Lane
Palo Alto, CA 94303

Summary: Computer Science Ph.D. with deep experience in natural language processing, machine learning, and approximate record matching. Business skills include 8 years' experience founding and growing a technology startup.

EXPERIENCE

SPOCK NETWORKS, Redwood City, CA

May, 2007 – Present

Principal Scientist

- Play key scientific role in rapidly-growing early-stage people search engine:
 - Research and develop processes to extract biographical information about people from diverse public websites for the purpose of generating profiles for the Spock website
 - Research and develop process to link profiles of people so that the Spock website will have only one profile for each real-world individual

CHOICEMAKER TECHNOLOGIES, INC., New York, NY

CTO

August 2006 – May, 2007

- Conceived, coordinated, and implemented a wide range of R&D projects:
 - Built probabilistic models using maximum entropy machine learning technology
 - Researched new approaches to approximate string matching
 - Researched and coded new algorithms for enhancing the functionality and robustness of ChoiceMaker's record matching processes

CEO

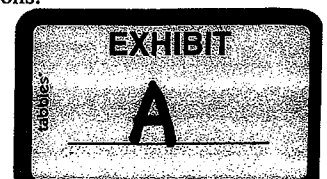
July 1998-August 2006

Business Accomplishments

- Founded the company to commercialize a machine learning approach to the problem of approximate record matching based on my Ph.D. research. For instance, our software can determine that records for "Andrew Borthwick" and "Andy Barthwick" represent the same person.
- Coordinated the successful deployment of systems with the Centers for Disease Control, New York City Department of Health, NY, IA, KS, MO, NE, NM, PA, SC, and WY State Education Departments, Regulatory DataCorp, Phoenix-ESI, and other clients.
- Hands-on work in marketing, including helping to develop marketing collaterals and the creation of design and content for the website.
- Actively involved in sales, including technical sales support and contract negotiation.
- Managed the firm's finances. Carefully monitored cash flow to enable firm to grow on minimal equity investments. Secured equity, debt, and government grant financing for the firm.
- Led all HR activities, including hiring, evaluation, and dismissal.

Technical Accomplishments

- Wrote papers and gave numerous presentations (including one invited talk) on record matching to help promote the firm.
- Principal investigator of three National Science Foundation Small Business Innovation Research grants. Grants provided \$1M for research into machine learning approaches to approximate record matching, high speed record matching, and the design of the ClueMaker programming language for record matching.
- Awarded US Patent 6,523,019 for machine learning approach to record matching. Also awarded U.K. patent for same work.
- Principal designer of high speed algorithm for real time "blocking", the first stage of matching in which a database is searched for possible candidate matches. Real-time algorithm received U.S. Patent #7,152,060. Algorithm takes a completely different approach to this problem from the main line of published research.
- Managed the ChoiceMaker product. Conceived and implemented a strategy which led to the construction of the "ChoiceMaker Developer" IDE for the creation and testing of record matching models and the "ChoiceMaker Server" system which our clients deploy in production.
- Personally coded ChoiceMaker version 1.0 in C++ using a flexible object oriented framework to describe the features, histories, and futures making up the system. Made heavy use of the STL. Used Perl for scripting the core modules. Deployed the system to the New York City Department of Health for use in production.
- Built a maximum entropy "estimator" in C++ for computing the weight to be used for features in a maximum entropy model. Estimator was used in ChoiceMaker 1.0, CM 2.0, and was licensed to two Japanese research institutions.



MORGAN STANLEY, New York, NY 1993-2002

Systems Consultant

- Working only one day per week, was critical designer and maintainer of the Information Services Allocation Model (ISAM). ISAM is a highly sophisticated system which solves matrix algebra equations describing the circular movement of money within IT in order to equitably allocate over \$1 billion in annual IT costs to the rest of the firm.
- Designed most of the major and minor upgrades for ISAM, which were implemented by a team of three full-time programmers. The system grew greatly in functionality and importance over nine years.
- Duties included making presentations to explain the functionality of the existing system, clarifying user requirements, designing enhancements, answering user questions, fixing bugs, and Y2K.
- One of a small number of consultants put on a *must-retain* list during a switchover of consulting agencies.

IBM WATSON LABORATORY, Yorktown Heights, NY Summer 1997

Summer Intern

- Researched maximum entropy language modeling for a voice-operated air travel reservation system.

MORGAN STANLEY, New York, NY

1988-1993

Programmer/Team Leader/Business Analyst

- Designed and managed the project which built ISAM.
- Supervised a team of four while working closely with the users in IT Finance to take the project from a few pages of notes, diagrams, and equations to a finished product.
- Personally coded the mathematical heart of the system in APL.

EDUCATION

Courant Institute of Mathematical Sciences, New York University, New York, NY

September 1999

- M.S. and Ph.D., Computer Science
- Thesis title: "A Maximum Entropy Approach to Named Entity Recognition"
- Specialized in Machine Learning and Natural Language Processing
- Advisor: Prof. Ralph Grishman
- 3.74 GPA
- Invented and constructed a system to detect proper names ("named entities") in newspaper text. Built the first system to combine the output of multiple hand-coded information extraction systems within a maximum entropy framework. System placed fourth out of twelve in a DOD evaluation after only four person-months of effort. Rapidly ported the system to Japanese and performed well in a Japanese named entity evaluation, where it was the only system written by a non-speaker of Japanese.

Oberlin College, Oberlin, OH

May 1988

- Bachelor of Arts, History
- 3.64 GPA
- Phi Beta Kappa
- Comfort Starr Prize for Excellence in History

PUBLICATIONS: Data quality and record matching

Patents

- Andrew Borthwick, Martin Buechi, and Arthur Goldberg. *Automated Database Blocking and Record Matching*. U.S. Patent #7,152,060. Filed April 11, 2003. Awarded December 19, 2006.
- Andrew Borthwick. *A Probabilistic Record Linkage Model Derived from Training Data*. U.S. Patent #6,523,019. Filed Oct. 28, 1999. Awarded February 18, 2003. Also awarded U.K. Patent #2,371,901.
- Co-inventor of one other pending patent.

Papers

- Andrew Borthwick. *The ChoiceMaker 2 Record Matching System*. ChoiceMaker Technologies white paper. November, 2004.
- Vikki Papadouka, Paul Schaeffer, Amy Metroka, Andrew Borthwick, Parisa Taranifar, Jessica Leighton, Angel Aponte, Runo Liao, Alexandra Ternier, Stephen Friedman, and Noam Arzt. *Integrating the New York City Immunization Registry and the Childhood Blood Lead Registry*. Peer reviewed paper. Journal of Public Health Management and Practice. November, 2004.

- Andrew Borthwick and Maggie Soffer. *Business Requirements of a Record Matching System*. Peer reviewed paper. Massachusetts Institute of Technology's Ninth International Conference on Information Quality (MIT ICIQ), Cambridge, MA. September 7, 2004.
- Martin Buechi, Andrew Borthwick, Adam Winkel, and Arthur Goldberg. *ClueMaker: A Language for Approximate Record Matching*. Peer reviewed paper. Massachusetts Institute of Technology's Eighth International Conference on Information Quality (MIT ICIQ), Cambridge, MA. August 27, 2003.
- Andrew Borthwick, Martin Buechi, and Arthur Goldberg. *Key Concepts in the ChoiceMaker 2 Record Matching System*. Peer reviewed paper. First Workshop on Data Cleaning, Record Linkage, and Object Consolidation, in conjunction with the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), Washington, DC. July 17, 2003.

Miscellaneous

- Andrew Borthwick. Expert witness testimony on record matching issues. *Washington Association of Churches, et. al. v. Reed*. May 24, 2006. Prepared in association with the Brennan Center for Social Justice and pro bono attorneys from Paul Weis. Resulted in an injunction brought against Washington State to block inaccurate record matching from being used on voter registration rolls. See www.choicemaker.com/content/news/press/20061009_testimony.php3 for details and www.brennancenter.org/dynamic/subpages/download_file_36559.pdf for my testimony.
- Andrew Borthwick. *When Accuracy Counts*. Podcast interview with Claudia Imhoff of the Data Warehouse Institute. May, 2006.
- Andrew Borthwick. *The Design and Testing of a Record Matching System*. Slides and abstract. 17th Information Quality Conference. Houston, Texas. September 21, 2005.
- Andrew Borthwick. *Record Linkage Industrial Trends*. Invited talk. First workshop on Data Cleaning, Record Linkage, and Object Consolidation in conjunction with the ACM SIG KDD's Ninth International Conference on Knowledge Discovery and Data mining. Washington, D.C., August 27, 2003.
- Andrew Borthwick and Deborah Walker. *Applications of Record Matching Techniques for a Lead-Immunization Registry Integration Project*. "35th National Immunization Conference", Slides and abstract, Atlanta, Georgia, May 2001.

PUBLICATIONS: Computational Linguistics

Links to all of the below can be found at scholar.google.com

- Andrew Borthwick. *A Maximum Entropy Approach to Named Entity Recognition*. Ph.D. thesis, New York University, New York, New York, September 1999.
- Andrew Borthwick. *A Japanese Named Entity Recognizer Constructed by a Non-Speaker of Japanese*. "Proceedings of the IREX Workshop", Tokyo, Japan, August 1999.
- Andrew Bothwick, John Sterling, Eugene Agichtein, and Ralph Grishman. *Exploiting Diverse Knowledge Sources via Maximum Entropy in Named Entity Recognition*. "Proceedings of the Sixth Workshop on Very Large Corpora", August 1998.
- Andrew Borthwick, John Sterling, Eugene Agichtein, and Ralph Grishman. *NYU: Description of the MENE Named Entity System as used in MUC-7*. "Proceedings of the Seventh Message Understanding Conference (MUC-7)", Fairfax, Virginia, April 1998.

TECHNICAL EXPERTISE

Operating Systems

- Windows, Unix/Linux, MVS (IBM Mainframe)

Technologies

- Data quality, record matching (a.k.a. "entity resolution", "deduplication", "record linkage"), high speed processing of large databases, computational linguistics, algorithms, software architecture, compilers

Programming Languages

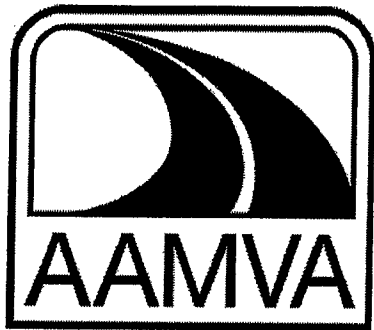
- Java, Python, ClueMaker[®] (Co-Inventor of proprietary language), C++ (including Standard Template Library), Perl, C, Adabas/Natural, APL

Software Packages

- ChoiceMaker 2, Eclipse, MS Project, Visio, QuickBooks, MS Office

Foreign Languages

- Reading knowledge of French, some German



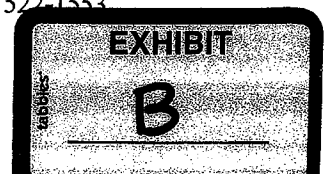
**American Association of
Motor Vehicle Administrators**

Social Security Verification (SSV)

System Specification

Release 2.0.0

August 2004



The American Association of Motor Vehicle Administrators (AAMVA) produced this document.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage or retrieval systems, for any purpose other than the intended use by AAMVA, without the express written permission of AAMVA.

©2004 AAMVA All rights reserved.

Table Of Contents

| | | |
|-------|--|----|
| 1 | INTRODUCTION | 5 |
| 1.1 | Document Objective | 5 |
| 1.2 | Getting Help (1-888-AAMVA-80) | 5 |
| 2 | APPLICATION DESCRIPTION | 6 |
| 2.1 | Social Security On-line Verification (SSOLV) | 6 |
| 2.2 | Help America Vote Verification (HAVV)..... | 6 |
| 3 | IMPLEMENTATION PLANNING | 7 |
| 3.1 | Requirements Definition..... | 7 |
| 3.2 | Design | 7 |
| 3.3 | Development..... | 7 |
| 3.4 | Testing..... | 8 |
| 3.4.1 | Internal Tests..... | 8 |
| 3.4.2 | Casual Testing..... | 8 |
| 3.4.3 | Structured Testing..... | 8 |
| 3.5 | Production Implementation..... | 9 |
| 3.6 | SSV Help Desk | 9 |
| 3.7 | Agreements | 10 |
| 4 | SYSTEM ARCHITECTURE | 11 |
| 4.1 | Basic SSV Configuration..... | 11 |
| 4.2 | Teleprocessing Monitor | 11 |
| 4.3 | Network Control Software (NCS) | 11 |
| 4.4 | AAMVAnet Message Interchange Envelope (AMIE) Structure..... | 12 |
| 4.4.1 | Background..... | 12 |
| 4.4.2 | Message Addressing | 13 |
| 4.4.3 | General Rules for AMIE Message Composition | 14 |
| 4.4.4 | Application Text Blocks | 15 |
| 4.4.5 | Message Format of Fields..... | 16 |
| 4.5 | Error Handling Specifications..... | 16 |
| 4.5.1 | Network Errors..... | 17 |
| 4.5.2 | System Errors..... | 17 |
| 4.5.3 | Processing Errors | 18 |
| 4.6 | Application Layer Network Interface Software..... | 18 |
| 4.6.1 | AAMVA's Unified Network Interface (UNI) | 18 |
| 4.6.2 | Message Retry..... | 18 |
| 4.6.3 | Hard Manual Down..... | 19 |
| 4.6.4 | Message Locator | 19 |
| 4.6.5 | Call List..... | 20 |
| 4.6.6 | Driver Call List Layout..... | 20 |
| 4.6.7 | UNI Platforms Supported | 20 |
| 5 | SSV TRANSACTIONS..... | 21 |
| 5.1 | Social Security On-line Verification (SSOLV) Tansaction..... | 21 |
| 5.1.1 | 'SS' - SSA Verification Request Message..... | 21 |
| 5.1.2 | 'HS' - SSA Verification Response Message..... | 23 |
| 5.2 | Help America Vote Verification Transaction | 25 |

| | | |
|--|--|----|
| 5.2.1 | 'IH' - HAVA Verification Request Message..... | 25 |
| 5.2.2 | 'RH' - HAVA Verification Response Message..... | 26 |
| APPENDIX A - DATA ELEMENTS BY MESSAGE TYPE | | 28 |
| | SS - SSA VERIFICATION REQUEST (1751)..... | 31 |
| | HS - SSA VERIFICATION RESPONSE (1752)..... | 32 |
| | IH - HAVA VERIFICATION REQUEST (1761)..... | 33 |
| | RH - HAVA VERIFICATION RESPONSE (1762) | 34 |
| APPENDIX B - BLOCKS BY MESSAGE TYPE..... | | 35 |
| APPENDIX C - DATA ELEMENTS BY BLOCK..... | | 37 |
| APPENDIX D - DATA DICTIONARY..... | | 41 |
| | APPENDIX D.1 - DATA ELEMENTS..... | 41 |
| | APPENDIX D.2 - SSA Name Formatting Rules..... | 47 |
| APPENDIX E - CALL LIST | | 52 |

1 INTRODUCTION

1.1 Document Objective

The purpose of this document is to describe the data flows and transactions in the Social Security Verification application. The document is written for the Social Security Administration (SSA) and Jurisdictions who must develop Social Security On-line Verification (SSOLV) and Help America Vote Act Verification (HAVV) systems. The document contains the information necessary for a software application development team to:

- Write an implementation plan;
- Determine requirements for their application, based on nationwide requirements;
- Construct a framework for the design of their system implementation.

Because the requirements are written at a high level, a detailed implementation specification should be produced by the developers to describe how the system will be implemented in their environment.

The original release of this document focused on SSOLV implementation at SSA. This release also contains information for users who make SSOLV inquiries to SSA and a full description of the HAVV transaction.

1.2 Getting Help (1-888-AAMVA-80)

Questions regarding this document or the application itself should be directed to:

Operations Department:

Hours: 8:00 a.m.- 6:00 p.m. Eastern Time
Telephone: 1-888-AAMVA-80
Fax: (703) 522-1553
Address: AAMVA, Inc.
4301 Wilson Boulevard, Suite 400
Arlington, Virginia 22203
Website: www.aamva.org
e-mail: opsdept@aamva.org

2 APPLICATION DESCRIPTION

The Social Security Verification application (SSV) consists of two transactions: the Social Security On-line Verification (SSOLV) and the Help America Vote Verification (HAVV). Each transaction contains two messages: an inquiry message sent to the Social Security Administration (SSA) and a response message returned by the SSA.

2.1 Social Security On-line Verification (SSOLV)

Driver licenses and identification cards issued by US Motor Vehicle Agencies (MVA's) have become the U.S. standard for identification. In order to curb the fraudulent issuance of driver license and identification cards, the MVA's carefully review documentation that is presented to them to verify the identity of the individual. The Social Security Card is one form of identification that is reviewed. In most jurisdictions, the Social Security Number (SSN) is also used as the standard to uniquely identify individuals on the licensing records.

To minimize the fraudulent issuance of the driver license or identification card, the MVA's need a way to verify the information contained on the card is valid. The SSN verification needs to be performed on-line while the applicant is still at the MVA counter but prior to the issuance of the driver license or identification card.

The Social Security On-line Verification (SSOLV) transaction has been developed to allow authorized MVA's to have on-line access to SSA for SSN verification. Using this transaction, a MVA electronically sends SSA a person's name, date of birth (DOB) and SSN. SSA then compares this data to what is on its Master File. SSA will then respond back to the inquiring MVA, indicating how much of the MVA-submitted data matched against the SSA file.

2.2 Help America Vote Verification (HAVV)

Section 303 of Public Law 107-252 (Help America Vote Act of 2002) requires States and localities to develop centralized, computerized voter databases and to verify voter registration information. Individuals registering to vote must provide their driver's license number to the State election agency. If the registrant has no driver's license, they must supply the last four digits of their SSN. The statute requires that the chief State election official and the officials responsible for the State motor vehicle authorities to enter into agreements to match voter registration information with MVA information. The statute further requires the MVA officials and the Commissioner of Social Security to reach agreements for the purpose of verifying name, date of birth, the last four digits of the SSN, and any information recorded in SSA's records about the death of an individual.

The Help America Vote Verification (HAVV) transaction allows a MVA to submit an inquiry to SSA. The SSA verifies the information and responds back to the MVA with the results.

The Primary Address is the 2-character code for jurisdictions and AAMVA processing sites (normally the postal abbreviation for jurisdictions), and the Interface Code is used to distinguish between multiple systems at a single site. For example, in some states the driver licensing and vehicle registration systems are operated on different physical machines. The Interface Codes would be different for each.

AAMVA manages the overall AMIE UserID system, and is therefore responsible for assigning all values as necessary for the GAP Code.

The User Extension field of the Primary User description can be used at the discretion of the users, within the normal parameters for AMIE Messages (See the section on General Rules for AMIE Message Composition). This field is frequently used to identify a particular workstation that originated the message and therefore should receive the response. Other uses are possible depending on the needs of the users. Usage of this field should be limited to the Transaction Originator because it is the pass-through field.

4.4.3 General Rules for AMIE Message Composition

Data in an AMIE message may consist of any printable character. This means that non-printable bytes are not allowed in any AMIE message. This limitation has been imposed due to the architecture of the AAMVAnet network, which consists of many different types of computers on the network, each possibly having a different data-encoding scheme.

For example, the AT&T NETWORK SERVICES and its mainframes store character data in EBCDIC, while Unisys, Bull, and most other computer types store character data in ASCII. Translation between these code sets is performed as part of the network transmission to or from an ASCII based machine. The translation occurs by replacing a bit pattern from one code set with the corresponding bit pattern from the other code set. As the translation is performed to each byte of data traveling on the data path without regard to the content of the data, non-printable data would be corrupted when the bit patterns were replaced as if the byte contained character data.

Translation adulteration aside, each different machine type stores computational numeric data in a format native to the processor. Assuming numeric data could move between AAMVA nodes without adulteration, the data would probably be unusable by the destination node unless the origination and destination nodes happen to be compatible machine types.

For example, floating point decimal data on an AT&T NETWORK SERVICES mainframe is stored in a specific pattern of bits within two, four, or eight bytes, depending on the resolution required. Elements such as the exponent and mantissa are assigned to certain bits and are represented in defined ways. The same number on a VAX machine is stored with a different bit pattern, different exponent bases, and different byte order. Moving a floating-point decimal data item from an AT&T NETWORK SERVICES platform to a VAX would not yield usable data on the VAX. The reverse is also true.

Eventually, exceptions to this rule may be required to allow movement of complex data in an efficient manner, possibly using encoding and compression schemes. At that time specific exceptions will be defined and will be documented to an extent that potentially affected users will be aware of their limitations. However, the general rule will still apply to all other messages that may be sent between nodes running on different computer types.

To ensure only printable bytes exist in a message, you must initialize all unused areas of each block with spaces. This ensures that un-addressable areas, such as the reserved bytes at the end of most, contain valid AMIE data. The unused fields should also be initialized to spaces regardless of the data type of the field. For example, a date field is normally numeric, yet if the field is not a valid part of the message being built, the field should contain spaces rather than zeroes. Do not initialize AMIE blocks or fields to LOW-VALUES or HIGH-VALUES, as these are binary zeroes or ones, respectively, and do not represent printable data.

All application data elements must contain printable characters that can be used in both ASCII and common versions of EBCDIC. The printable characters are:

```
space
a to z
A to Z
0 to 9
! " # $ % & ' ( ) * + , - . / : ; < = > ? @
```

Other characters are not printable in ASCII and US-EBCDIC, so should be excluded. The user will need to determine if the non-printable characters will be omitted or if they will substitute another character. The recommendation for the Spanish 'Ñ' and 'ñ', is to convert the character to 'N' and 'n' before sending the data.

4.4.4 Application Text Blocks

For this system, the text block pool of an AMIE message contains the following block types:

- Message Exchange Control block (02/2). One Message Exchange Control (MEC) block will be present on each message. See the Message Exchange Control Block section for details.
- Business Application blocks (09/1, 10/1).
- Return-as-received blocks (98/3). Zero to five return-as-received blocks may be used, and they are used by the transaction originator.
- Error blocks (99/1). Zero to five error blocks are used, depending on the number of errors detected. See the Error Handling Section for details.

Because the blocks are sent in the Type/Sub-type number order, the text blocks will be sent in the order shown above.

Most blocks are used once within a message. However, instances exist where an AMIE text block is used multiple times within a message. These multiple repetitions exist when:

- A field is too long to fit in a single 61-byte block. A 108-byte address is transmitted in two AMIE text blocks. The first 61 bytes are sent in the first block and the final 47 bytes are sent in the second block.
- The application data is needed multiple times, where a single occurrence of the data will fit onto one block. The number of blocks will correspond to the number of occurrences of the data. The data is needed multiple time times; however, the total length of the data to be repeated exceeds one block. In these situations, the number of AMIE text blocks used is the product of the number of blocks used to hold a single occurrence, times the number of occurrences.

To be unique the Text Block Key will use an incremented line number to distinguish between the multiple occurrences of block types and maintain the sort sequence.

4.4.5 Message Format of Fields

All dates sent in the application specific blocks of the messages are passed as eight character fields in 'ccyymmdd' form, (e.g., '19951231'). All numbers sent in a message are passed in an unpacked form with leading zeros (e.g., a field with 6 integer digits with a value of '1,234', is transmitted as '001234', in an alpha numeric field).

For elements that require specific values (such as codes), the fields transmitted must contain the standard values, as defined in the data dictionary.

4.5 Error Handling Specifications

The error handling procedure describes a convention by which every message error will be processed, both by the entity that detected the error and the entity that originated the message. The errors can be categorized as follows:

- network errors;
- system errors, such as program aborts, files off line, or similar conditions;
- processing errors which are caused by faulty application data in the message

When an error is detected, the message that encountered or contained the error is returned to the sender. There are several flags and fields in the message structure that can convey information regarding errors or unusual circumstances. Depending on the severity of the problem, different combinations of the error flags/fields are used. Information can be found in the following areas:

GNCBER - NCB ERROR CODE

Set to 'Y' (yes)

GNETST – NETWORK STATUS

Set to a value other than zero, that describes the error.

GAPPST - APPLICATION STATUS

Set to a value other than space or zero, that describes the error.

GERUEC – UNI ERROR CODE or GERCDO – ERROR CODE

Set to a value other than space, that describes an error.

GERMSO - ERROR MESSAGE DESCRIPTION

A 54 character text field containing the description of the error.

4.5.1 Network Errors

Network errors occur when the origination or destination entity drops from the network or the network itself encounters a failure. There are established availability requirements that minimize occurrences of this nature, but occasionally a failure occurs.

When the originating entity is not connected or the network is completely down, the error is normally detectable and the message can be set-aside for later transmission. The Unified Network Interface (UNI) provides this service.

If the destination node is down, the network (NCS) will return the message to the originator with an indication of the error (NCB error code = 'U' for Undeliverable) and the message can be set aside for later transmission. If the destination application is down, UNI can detect the error, notify the originator, and set aside the message for later transmission.

4.5.2 System Errors

In this application system errors may be reported in one of two ways:

- Generic system errors
- SSA file off-line

A generic system error is an error with the system itself, such as program problems, network interface errors, database errors, program aborts, etc. To the extent possible, message recipients should try to detect these conditions and return the original message with the appropriate indicators to inform the originator of the problem (NCB error code = 'Y', processing status = '01', error block attached indicating the error and application status set to appropriate code, if applicable).

The more common system error occurs when the SSA file is off-line. In this instance, the SSA application will return the SSA Verification Response (HS) message with the SSA Verification Response Code set to '9'. Other system errors detected within the SSA application will also be reported with the Response Code set to '9' on the Verification Response message.

4.5.3 Processing Errors

The SSA will not edit data received in the incoming Verification Request (SS) nor will it return corrected information. Therefore, the only error a SOI should encounter would be that of a network or system error.

4.6 Application Layer Network Interface Software

The Application Layer Network Interface Software (ALNIS) is generically defined as a software application residing on the host computer. The main function is the translation between the AMIE message structure and a data element and the message structure used by the application. The application data structure is provided in COBOL and C formats. It also provides a variety of other application interface support features. The interface between the application and the ANLIS is usually platform dependent. An example of ALNIS software is AAMVA's Unified Network Interface (UNI) software package.

4.6.1 AAMVA's Unified Network Interface (UNI)

Unified Network Interface (UNI) provides critical services for jurisdictions' applications. The UNI was developed by AAMVA for its customers running applications requiring data transfer in the AAMVAnet Message Interchange Envelope (AMIE) electronic data interchange (EDI) format. Although using AAMVA's network interface tool is not a requirement, most users will choose to implement the system using the Unified Network Interface (UNI). UNI has several valuable functions available to assist users (such as message control, routing validation, logging, audit trails, and message grouping). A jurisdiction's network interface team needs to understand UNI's functions to avoid duplicating those functions within the application.

The purpose of this section is to supplement the UNI documentation by calling attention to several UNI features that have been found particularly useful. Although they are documented in the UNI Application Developer's Reference, we have included a brief synopsis here along with suggested settings, where applicable.

4.6.2 Message Retry

AAMVA recommends that users configure the parameter list of all on-line update messages to attempt up to three retries in the event the messages are undeliverable. When set, UNI retry is performed automatically. Users should keep in mind that automatic retry may not be appropriate for messages where the state prefers to control retries either manually or programmatically through the application (as may be the case with inquiry messages).

The PARM-CNT-RETRY-MAX field in the UNI parameter list controls the maximum number of times that UNI will attempt to send an outbound message to its destination. This is a 1-digit numeric field, so valid values range from '0' to '9'.

If the number of retries is set to '0' and the outbound message is returned as undeliverable, UNI will not retry the message. If the number of retries is set to a non-zero value, UNI will hold the message in its undeliverable message file until such time as UNI determines that the destination's node or application is again available. UNI actively checks the status of retry destinations and does not attempt a retry until a positive status is attained. UNI checks the status of all other nodes on the network by issuing IN messages at regular intervals and interrogating the RN responses. The default interval is 20 minutes, but this is configurable. UNI will attempt to resend until it has exhausted the maximum number of retries designated.

4.6.3 Hard Manual Down

A hard manual down causes UNI to treat a destination node as though it were down even when it is not. This can be used, for example, when a state must store on-line transactions while its load file is being processed. Issuing a hard manual down on the destination node causes on-line transactions to that node to go to the message pending process given message retry is configured. Transactions will continue to queue up in message pending until the hard manual down is manually removed. As stated earlier, it is very important to pace messages being released from message pending.

Hard manual downs are issued from the UTT200 Network/Application Status screen by adding the site ID of the destination to be downed to the application status list. First, enter an action code of 'A', the network ID of the destination, and an application code of '11'. The down reason will be set to 'soft manual' by the system. To change the down reason to 'hard manual', enter an action code of 'M'. The 'M' action code toggles between a soft and a hard manual down. To delete a hard manual down, enter an action code of 'D'. Message pending will initiate release of messages at the next IN/RN interval.

Before issuing a hard manual down, states should estimate the amount of space needed to store the message pending file. Steps should be taken to ensure that enough space will be available to hold the estimated number of pending messages.

4.6.4 Message Locator

When a transaction is initiated, UNI generates a unique identifier for the message called a message locator. UNI uses the message locator to match messages with their responses. When contacting the AAMVA Operations help desk for support, it is important that you provide the message locator. The message locator provides a means for the AAMVA Operations help desk to find the specific message or messages causing the problem.

The message locator is found in the first 26 bytes of the MEC block. It is comprised of a date/time/sequence number along with the message type.

A sample message locator and its components are shown below:

```
000502132312001    1UNISS
```

where:

'000502' is the date

'132312' is the time

'0001' is the sequence number

' ' is a constant

'1' is the occurrence of the destination in the PARM-DESC-TABLE-DEST of the parameter list

'UNI' is a constant

'SS' is the message type

4.6.5 Call List

UNI provides a parameter list and call list to interface between the jurisdiction's application and the network. The call list data is converted to the AMIE structure before it is sent to network and vice-versa. The parameter list provides a means for matching response messages to inquiry messages, routing messages and store and forward features. The parameter and call lists use a flat file format which make it easy for developers to address the elements.

4.6.6 Driver Call List Layout

In the Driver Call List, there is a record type indicator (CLMF-DESC-RECORD-TYPE) that is populated by UNI when a message is received. This indicator is used to identify how much of the variable length Call List is being used. In this application UNI sets the indicator to "R", "L" or "S". When the indicator contains a:

"L" the type of record is a long record. In this situation the address is included.

"S" the type of record is a short record. In this situation no address is included.

"R" the type of record is a return as received.

So before addressing elements residing in the extended part of the call list, check the record type indicator to ensure a long call list has been delivered.

4.6.7 UNI Platforms Supported

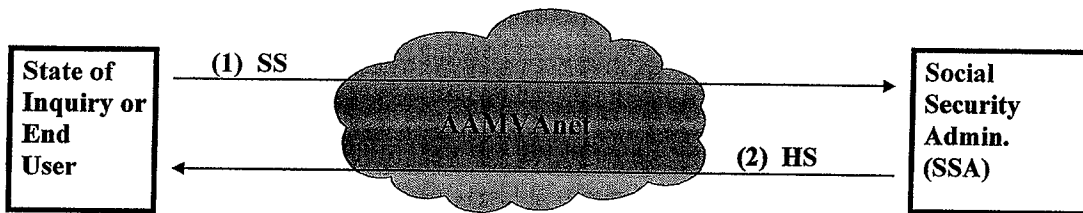
AAMVA's web site (www.aamva.org) has a complete up-to-date listing of supported platforms.

5 SSV TRANSACTIONS

5.1 Social Security On-line Verification (SSOLV) Transaction

Purpose: The SSOLV Transaction is used by an authorized MVA (End User) to request the verification of an SSN provided by an applicant or that is found on the MVA's database to aid in the prevention of fraudulent identification issuance.

Transaction Message Flow Diagram



1. The MVA (End User) formats the request into the AMIE format and forwards the it to the SSA through the AAMVAnet network.
2. SSA receives the request and responds to the State of Inquiry (SOI) with the verification data in the AMIE format.

Note. For detailed information on the message formats, the AMIE blocks and the data elements, refer to Appendixes A, B, C and D.

5.1.1 'SS' - SSA Verification Request Message

5.1.1.1 State of Inquiry (SOI) Processing Requirements:

The SOI must provide the following data elements to successfully process the SSA Verification Request (SS):

- Social Security Number (DDVSSN) Required
- Driver Name (DDVNM4) Required (See the SSA Name Formatting Rules in the Appendix)
- Driver Date of Birth (DDVDOB) Required

In addition the SOI may include the following elements:

- Jurisdiction (DDLJU1) Optional

- Driver License Number (DDLNUM) Optional
- Return as Received (GRREC2) Optional

NOTE: Do not attempt to verify SSNs allocated by user applications (e.g. the CDLIS substitute and pseudo-SSN), because the SSA will always respond that such SSNs are invalid.

5.1.1.2 Social Security Administration (SSA) Processing Requirements:

Upon receiving the SSA Verification Request (SS), the Social Security Administration (SSA) will search for the requested record in its database.

NOTE: The SSA will not edit or check for errors in the SS message, it only verifies the data present.

5.1.1.2.1 SSOLV Name Match Criteria

A name (see the SSA Name Formatting Rules in the Appendix) provided by the MVA will be accepted as verified, if a match is made using any the following criteria:

1. If the first seven positions of the surname (e.g.: last name) and the first and middle name initials match exactly.
2. If only one initial is provided, the first seven positions of the surname must match and the initial provided will match the first initial of either the first or middle name.
3. The first four positions of the input first name and the first four positions of the file first name match.
4. If no first name is provided, the first four positions of the surname and the first and middle name initials must match.
5. A one letter difference or transposition of two adjacent letters in the first seven positions of the surname and the first and middle name initials match exactly (AB=AB) or are transposed (AB=BA).
6. A one letter difference or transposition of two adjacent letters in the first seven positions of the surname and
 - a) the first or middle initial of the MVA name match that of the first name initial of the SSA name when only one initial is present on SSA files (AB=A or BA=A); or
 - b) the first initial of the MVA name matches the first or middle initial of the SSA name when only one initial is present on the MVA record (A=AB; A=BA; B=BA; B=AB); or
 - c) the MVA first name initial matches the SSA first name initial and the MVA middle name initial disagrees with the SSA middle name initial, but matches the first initial of another

surname for a female (AB SM@TH = AG SMITH X REF - Brown, sex = female, i.e. a maiden name check).

7. An extraneous or missing letter is present in the first seven positions of the MVA surname and the MVA first name initial matches the SSA first or middle name initial.

| Extraneous Letter | | Missing Letter | |
|-------------------|----------------------|----------------|-----------------------|
| A | JJOHNSO = A JOHNSON | AR | OHNSTON = A JOHNSTON |
| A | J@OHNSO = A JOHNSON | A | JHNSTON = A JOHNSTON |
| A | JOSHNSO = A JOHNSON | A | JONSTON = A JOHNSTON |
| B | JOHHNSO = AB JOHNSON | A | JOHSTON = A JOHNSTON |
| B | JOHNOSO = AB JOHNSON | B | JOHNTON = AB JOHNSTON |
| B | JOHNSTO = AB JOHNSON | B | JOSHSTN = AB JOHNSTON |

8. A compound surname may only be verified using one surname. If the single MVA surname contains more than three letters SSA will compare it to up to 13 positions of the SSA name. SSA will compare positions 1-7, then 2-8, then 3-9, then 4-10, then 5-11, then 6-12, and finally 7-13. If a match occurs on any one of these comparisons, the compound surname will be verified.

5.1.1.2.2 SSOLV Date of Birth (DOB) Match Criteria

A DOB will be verified if it matches the SSA DOB using the following criteria:

1. The year of birth on the MVA record matches the year of birth on the SSA record exactly. The day and month are ignored.
2. The year of birth on the MVA record differs from the SSA DOB +/- one year and the month on the MVA record matches the SSA month.

5.1.1.2.3 SSOLV SSN Match Criteria

The SSN sent on the verification request will only be reported as verified if it matches the SSN found on the SSA record exactly.

5.1.2 'HS' - SSA Verification Response Message

5.1.2.1 Social Security Administration (SSA) Processing Requirements:

After checking for a record in its database, the SSA will send the SSA Verification Response (HS) message to the SOI with the SSA Verification Response Code (GMSVRC) in the MEC block.

The following is a list of SSA Verification Response Codes returned and a description of their meaning:

| <u>Code</u> | <u>Description</u> |
|-------------|---|
| 1 | SSN, Name and DOB verified |
| 2 | Invalid SSN |
| 3 | Name did not verify, DOB is valid |
| 4 | DOB did not verify, Name is valid |
| 5 | Name and DOB did not verify |
| 6 | Unable to process request - go to the local Social Security office for more information |
| 9 | System Error. Unable to process at this time |

5.1.2.2 State of Inquiry (SOI) Processing Requirements:

The SOI should examine the SSA Verification Response Code (GMSVRC) on the HS message.

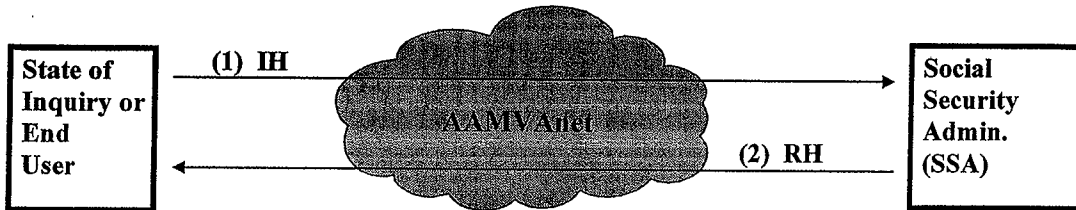
If the driver identification information is verified and the applicant has nothing on his/her record to prevent the issuance/renewal of a license the application/renewal may be processed.

If the information provided by the applicant does not verify, the MVA will utilize jurisdiction specific procedures for handling the applicant.

5.2 Help America Vote Verification Transaction

Purpose: The HAVV transaction is used by an authorized MVA (End User) to request the verification of a name, date of birth and a partial SSN (last four digits) provided by an applicant to aid in the prevention of fraudulent voter registration.

Transaction Message Flow Diagram



1. The State of Inquiry (MVA) formats the request into the AMIE format and forwards it to the SSA via the AAMVAnet network.

2 The SSA receives the request and responds to the State of Inquiry (SOI) with the verification data in the AMIE format.

NOTE:For detailed information on the message formats, the AMIE blocks and the data elements used in HAVV, refer to Appendixes A, B, C and D. For detailed information on interfacing your application to AAMVAnet, refer to the Unified Network Interface Application Developers Reference Manual (available through the AAMVA Operations Department).

5.2.1 'IH' - HAVA Verification Request Message

5.2.1.1 State of Inquiry (SOI) Processing Requirements:

The SOI must provide the following data elements to successfully process the HAVA Verification Request (IH):

- Last four digits of SSN (DDVSLF) Required
- Name (DDVNM4) Required (See the SSA Name Formatting Rules in the Appendix)
- Date of Birth (DDVDOB) Required

In addition the SOI may include the following elements:

- Return as Received (GRREC2) Optional

This data will be validated by SSA, the edits performed are shown in the next section. Jurisdictions should ensure they do not send data that will fail these edits.

5.2.1.2 Social Security Administration (SSA) Processing Requirements:

Upon receiving the HAVA Verification Request (IH), the SSA will validate the contents of the message. If any of the following edit rules fail, the response will have the SSA Verification Response Code (GMSVRC) set to 'S', indicating "Invalid Data".

- The last four digits of the SSN must be a number in the range "0001" to "9999".
- The Date of Birth must be a valid date (though the day of birth is not used).
- The First Name must have:
 - A-Z in position 1.
 - Then in positions 2 through 15: A-Z, a single embedded hyphen, apostrophe or space.
 - Last character must be A-Z, an apostrophe or a space; unless the 14th position is A-Z, then the 15th position can be a hyphen, apostrophe, space or an alphabetic character
 - Consecutive embedded combinations of spaces, hyphen, and/or apostrophe are not permitted.
- Last Name must have:
 - A-Z in position 1.
 - Acceptable characters for position 2 through 20 are A-Z, a single embedded hyphen, apostrophe or space.
 - Last character must be A-Z, an apostrophe or a space; unless the 19th position is A-Z, then the 20th position can be a hyphen, apostrophe, space or an alphabetic character.
 - Consecutive embedded combinations of spaces, hyphen, and/or apostrophe are not permitted.

The name in the message will be in a packed form (see the SSA Name Formatting Rules in the Appendix for details).

Valid messages are then checked against the SSA database using the following elements:

| <u>Input</u> | <u>Match Criteria</u> |
|-----------------------------|---|
| Last Name | Exact |
| First name | Exact |
| Middle Initial | Ignore |
| Date Of Birth | Month and year must be exact. Ignore day. |
| Last four digits of the SSN | Exact |

5.2.2 'RH' - HAVA Verification Response Message

5.2.2.1 Social Security Administration (SSA) Processing Requirements:

After checking for a record in its database, the SSA will send the HAVA Verification Response (RH) message to the SOI with the Response Code in the MEC block.

The following is a list of the SSA Verification Response Codes (GMSVRC) returned for HAVV and a description of their meaning.

| <u>Code</u> | <u>Description</u> |
|-------------|---|
| S | Invalid input data |
| T | Multiple matches – all deceased |
| V | Multiple matches – all alive |
| W | Multiple matches – at least one alive (& at least one deceased) |
| X | Single match – alive |
| Y | Single match – deceased |
| Z | No match found |
| 9 | System Error. Unable to process at this time |

5.2.2.2 State of Inquiry (SOI) Processing Requirements:

The SOI should examine the SSA Verification Response Codes (GMSVRC) on the 'RH' message.

If the information provided by the applicant does not verify, the MVA will utilize jurisdiction-specific procedures for handling the applicant.

Florida Voter Registration System



Guide to FVRS

Version 1.0

September 7, 2005



Florida Department of State
Division of Elections
FVRS Project Office
409 East Gaines Street
Tallahassee, Florida 32399-0250
850.245.6229

Jeb Bush
Governor

Glenda E. Hood
Secretary of State

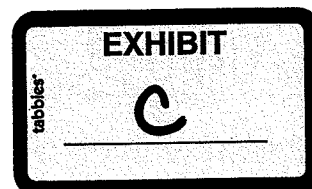


Table of Contents

| | |
|---|-----------|
| Table of Contents..... | i |
| List of Tables..... | v |
| List of Figures..... | vi |
| Part 1 – Introduction and Background..... | 1 |
| 1 Introduction..... | 1 |
| 1.1 Purpose..... | 2 |
| 1.2 Intended Audience..... | 2 |
| 2 FVRS Project Background..... | 3 |
| 2.1 Key Business Objectives..... | 3 |
| 2.2 Schedule of FVRS Project Activities..... | 4 |
| Part 2 – FVRS Design and Configuration..... | 5 |
| 3 FVRS Development Approach..... | 5 |
| 3.1 High-level Design and Requirements Assessment..... | 5 |
| 3.2 Procurement of Project Management and Quality Assurance Services..... | 5 |
| 3.3 Procurement of Prime Contractor/Systems Integration Services..... | 6 |
| 4 Major FVRS System Functions..... | 7 |
| 4.1 Online Transaction Processing (OLTP)..... | 9 |
| 4.1.1 FVRS Transactions..... | 9 |
| 4.1.2 FVRS Transaction Specifications..... | 10 |
| 4.2 Business Logic and Workflow Control..... | 11 |
| 4.3 Database Services..... | 11 |
| 4.4 Security and User Administration..... | 12 |
| 4.5 Data Warehouse..... | 12 |
| 5 FVRS Hardware and Software Configuration..... | 12 |
| 5.1 Production, QA/Test and Development Platforms..... | 13 |
| 6 FVRS Network and Communications..... | 14 |
| 6.1 Introduction..... | 14 |
| 6.2 Provided Bandwidth and Transmission Speeds..... | 14 |
| 6.3 General Configuration..... | 15 |
| 7 FVRS Security..... | 15 |
| 7.1 Security Approach Overview..... | 16 |
| 7.2 County System Security Administrator (SSA)..... | 17 |

7.3 Security Responsibilities of the State 17

7.4 Security Responsibilities of Counties..... 19

8 Remediation of County Voter Registration Systems.....21

8.1 Selection and Procurement of County Voter Registration System.....21

8.2 Additional Hardware and Software Requirements21

8.3 Expected Roles of Voter Registration Vendors.....22

9 Data Conversion23

9.1 FVRS Data Conversion Overview24

9.2 Data Migration Approach25

9.3 Resources26

9.4 Identification of Target Cut-off Dates for Data Conversion27

9.5 Formatting County Records27

9.6 Assignment of FVRS Voter ID Number to Voter Registration Records.28

9.7 Identification of Data Sources29

9.7.1 Voter Registration Records29

9.7.2 Voter Images29

9.7.3 Voter History.....31

9.7.4 Street and Address Information32

9.7.5 Petition Verification Records34

Part 3 – Operations Under FVRS35

10 Redesign and Re-issuance of Forms.....35

10.1 Voter Information Card35

10.2 Statewide Voter Registration Application.....35

11 Voter Registrations and Applications.....36

11.1 Registration Processing and Disposition Terms36

11.1.1 Application Processing Status36

11.1.2 Application Dispositions.....37

11.2 Voter Registration Status.....38

12 Voter Registration Processing by Counties40

12.1 Processing Registration Forms for Voters Outside of a County’s
Jurisdiction40

12.2 General Procedures41

12.3 New Voter Registration.....41

12.4 Updates to Existing Voter Registration Records.....47

12.5 Other Voter Registration Adjustments50

12.6 Other Voter Status Changes.....50

12.7 Suspense Applications50

12.7.1 Why Applications Become Suspended.....50

12.7.2 What Happens When an Application is Suspended51

| | | |
|-----------|--|-----------|
| 12.7.3 | How to Process a Suspended Application..... | 51 |
| 13 | Synchronization between FVRS and County Systems..... | 52 |
| 13.1 | Verifying Synchronization | 52 |
| 13.2 | All Values Verification | 54 |
| 14 | Match Processing and Determination of Eligibility | 54 |
| 14.1 | Duplicate Registrations | 55 |
| 14.1.1 | Identification of Duplicate Registrations Prior to January 2006 | 55 |
| 14.1.2 | Identification of Duplicate Registrations after Conversion and Cutover to Production..... | 56 |
| 14.2 | Deceased Voters | 57 |
| 14.3 | Identification of Potential Felons..... | 58 |
| 14.3.1 | New registrations or updates to existing registrations occurring after January 1, 2006..... | 58 |
| 14.3.2 | Updates to FDLE Felony Conviction Data | 58 |
| 14.3.3 | Felony Convictions after January 1, 2006 | 59 |
| 14.3.4 | Procedures Scheduled after November, 2006..... | 59 |
| 14.3.5 | Comparison with Office of Executive Clemency Records..... | 59 |
| 14.4 | Identification of Mental Incompetence | 59 |
| 14.5 | Match Verification by the Department..... | 60 |
| 14.5.1 | Department of Highway Safety and Motor Vehicles, Driver and Vehicle Information System..... | 60 |
| 14.5.2 | Department of Corrections | 60 |
| 14.6 | County Notification of Match Records | 60 |
| 14.7 | Update of Match Records | 61 |
| 15 | Precinct Registers | 62 |
| 15.1 | Existing Procedures and Challenges for the FVRS | 62 |
| 15.2 | FVRS Base Precinct Register - E-minus 15 | 63 |
| 15.3 | Register Supplements | 63 |
| 15.4 | Use of the Supplements | 64 |
| 16 | FVRS and Early Voting..... | 64 |
| 16.1 | Voter History Updates..... | 65 |
| 16.2 | Absentee Ballot Tracking..... | 65 |
| 17 | FVRS Notifications | 66 |
| 17.1 | Introduction to Notifications | 66 |
| 17.2 | Notification Retrieval Process | 68 |
| 17.3 | Frequency of Polling..... | 68 |
| 17.4 | Retrieving and Processing a Single Notification Message..... | 68 |
| 18 | Geographical Information Processing..... | 72 |

| | | |
|-----------|---|-----------|
| 18.1 | County Upload of Street Data | 72 |
| 18.2 | Frequency of Update | 72 |
| 18.3 | Redistricting and Reprecincting | 72 |
| 18.4 | Updating FVRS for Redistricting and Reprecincting | 73 |
| 18.5 | Spelling Changes for Street Names | 73 |
| 19 | Scheduling and Logging Correspondence with the Voter | 73 |
| 20 | Assignment of Precinct and Political Jurisdictions | 75 |
| 21 | Petition and Initiative Signature Verification | 76 |
| 21.1 | Introduction | 76 |
| 21.2 | January 1, 2007 Effective Date | 76 |
| 21.3 | State vs. Local Petition and Initiatives | 76 |
| 21.4 | Assignment of State Petition and Initiative Numbers | 77 |
| 21.5 | Signature Processing | 77 |
| 22 | County Readiness Tasks | 77 |
| 23 | Definition of Terms | 82 |

List of Tables

| | |
|---|----|
| Table 1 Conversion of Voter Registration Records by Type and Period | 29 |
| Table 2 Match Notification Types | 61 |
| Table 3 Notification Types | 67 |
| Table 4 FVRS Contact Types | 74 |
| Table 5 Communications with Voter Registration Updates | 75 |
| Table 6 Technical Terms | 82 |
| Table 7 Project Terms..... | 89 |

List of Figures

| | |
|--|----|
| Figure 1 FVRS System Functions | 8 |
| Figure 2 FVRS System Architecture | 13 |
| Figure 3 FVRS Security Architecture | 16 |
| Figure 4 Conversion Process Flow Overview | 28 |
| Figure 5 Voter Image Conversion Diagram..... | 30 |
| Figure 6 Voter History Conversion Flow Diagram | 31 |
| Figure 7 Street Segment Conversion Flow Diagram..... | 33 |
| Figure 8 Petition Conversion Flow Diagram..... | 34 |
| Figure 9 Typical New Voter Registration Process..... | 42 |
| Figure 10 FVRS Notification of Synchronization | 53 |
| Figure 11 Match Notification Process | 61 |

11 VOTER REGISTRATIONS AND APPLICATIONS

When a voter registration application is submitted to FVRS, it is held in an application table until the application has been completely processed. A voter who is already registered may, therefore, have an active registration record, and an unresolved application. This allows the official registration record to be maintained undisturbed while an application is being processed. Application records are linked to their parent voter record by the *FVRS Voter ID Number*. Each application record is further qualified by a sequence number assigned by FVRS upon receipt of an application.

This relationship between a voter record and one or more application records will also be implemented for new registrations where an existing voter record does not previously exist. Under this condition the relevant data elements from the application will be used to populate and create a voter record, generate a unique FVRS Voter ID Number and create an application record related back to the Voter Record.

11.1 REGISTRATION PROCESSING AND DISPOSITION TERMS

For the purpose of clarity, the following terms have a precise meaning in the context of FVRS.

11.1.1 Application Processing Status

An application processing status will be assigned to all voter registration applications submitted to and accepted by FVRS³. This designation defines a workflow or processing state and does not define an application's final disposition. An application's processing status may change during its life cycle. The discreet processing statuses and definitions to be managed by FVRS are described below.

| Status | Description |
|-----------|---|
| Suspended | Voter registration applications can be submitted to FVRS with a suspended status which will instruct FVRS not to apply further validity, verification or eligibility assessment procedures. A suspended application may be submitted by a county data entry operator for the purpose of later retrieval and completion of data entry or for the purpose of routing the application to another county for completion. Suspended applications should be attended to promptly by the assigned county to avoid delay in the registration process. |

³ Only applications which fail basic data validation rules will be rejected by FVRS and not assigned an FVRS ID number.

| Status | Description |
|---------|--|
| Pending | A new registration application is pending when it is received by FVRS and the application did not meet the criteria for a Denial or Incomplete disposition, and where the application is still being processed by the Department of State for the purpose of verification of Driver's License Number or Social Security Number conditions. |
| Closed | An application is closed when a disposition of the application is determined and assigned. The types of valid dispositions that may be assigned to an application are listed and described in Section 11.1.2 |

11.1.2 Application Dispositions

An application disposition will be assigned to all voter registration applications submitted to and accepted by FVRS for processing. This designation defines the standing of the **application** presented for processing and not necessarily the Voter Registration Status (see Section xxx) of the **registrant**. This distinction is important for applications received as updates for existing FVRS registrants. For instance, an "incomplete" application disposition for an existing eligible voter will not affect the registrant's current voter registration status. The discreet application dispositions and definitions to be managed by FVRS are described below.

| Disposition | Description |
|-------------|--|
| Denied | <p>Once an application is denied, the voter is provided a notification. The following are the reasons for an application being denied.</p> <ul style="list-style-type: none"> • Applicant was not 17 years old on the date of the application • The applicant is not a US Citizen <p>A denied voter is not sent an application form with a Denial letter since a new application will not cure the problem (with the exception of the under 17 voter, where time will take care of the problem.)</p> |
| Incomplete | <p>A voter registration application is complete if it contains the following information necessary to establish eligibility pursuant to s. 97.041:</p> <ol style="list-style-type: none"> 1. The applicant's name. 2. The applicant's legal residence address. 3. The applicant's date of birth. 4. A mark in the checkbox affirming the applicant is a citizen of the United States. 5.a. The applicant's current and valid Florida driver's license number or , the identification number from a Florida identification card issued under s. 322.051, or b. If the applicant has not been issued a current and valid Florida |

| Disposition | Description |
|-------------|---|
| | <p>driver's license or a Florida identification card, the last four digits of the applicant's social security number.</p> <p>c. In the case where an applicant has not been issued a current and valid Florida driver's license or Florida identification card or social security number, the applicant shall affirm this fact in the manner prescribed in the uniform statewide voter registration application.</p> <p>6. A mark in the checkbox affirming that the applicant has not been convicted of a felony or that, if convicted, has had his or her civil rights restored.</p> <p>7. A mark in the checkbox affirming that the applicant has not been adjudicated mentally incapacitated with respect to voting or that, if so adjudicated, has had his or her right to vote restored.</p> <p>8. Original signature or a digital signature transmitted by the Department of Highway Safety and Motor Vehicles of the applicant swearing or affirming under the penalty for false swearing pursuant to s. <u>104.011</u> that the information contained in the registration application is true and subscribing to the oath required by s. 3, Art. VI of the State Constitution and s. <u>97.051</u>.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. <i>An applicant whose application is denied is sent an incompleteness notice listing the reasons for the application not being processed and another application form so that a corrected application can be presented.</i> 2. <i>An application to update an existing registration that contains incorrect information or information that can not be verified may acquire an incomplete status. This will allow a notification to be generated, but will NOT alter the voter registration status.</i> 3. <i>A voter that has a registration status of Active, Inactive or Pre-Registered cannot be moved to a Denied status. If a voter becomes ineligible, an administrative process must be used to remove the voter.</i> |
| Registered | The voter's registration record has been updated with all possible information |

11.2 VOTER REGISTRATION STATUS

Each voter maintained in FVRS will be assigned a Voter Registration Status which will determine the voter's eligibility to vote. The Voter Registration Status will be updated after an application is processed (application processing status "closed") and an application disposition has been assigned. The discreet voter registration statuses and their definitions to be managed by FVRS are described below.

| Status | Description |
|------------|--|
| Active | The voter is properly registered. The voter is eligible to vote in elections. |
| Inactive | <p>There is one and only one way to acquire an inactive status. Each and every one of the following events must have happened in the correct order:</p> <ul style="list-style-type: none"> • The voter had an active status • First class mail was returned undelivered from the residence address of record for the voter • An "Address Confirmation Notice" has been sent to the voter • No response was received from the voter for 30 days following the sending of the Final notice <p style="margin-left: 40px;">1. <i>At this point the voter becomes Inactive. The voter is still eligible to vote in elections, and is included in the precinct register.</i></p> <p style="margin-left: 40px;">Any "voter activity" by the voter (which broadly is voting, or written contact from the voter, or signing a petition) will restore the voter to Active Status</p> <p style="margin-left: 40px;">After two general elections the voter is moved to the "Removed" status.</p> |
| Removed | <p>The voter is no longer eligible to vote in an election, and will not appear in the precinct register. There are a number of reasons why a voter can be removed:</p> <ul style="list-style-type: none"> • Failed to attend Admin Hearing • Office errors • Canceled • Deceased • Felon • Moved out of State. Request by voter • Adjudicated Mentally Incompetent • Office Duplicate Registration • Returned Mail, Inactive 2 yrs |
| Archived | Only voters with Removed Status can become Archived. The only purpose of doing this is to prevent long deceased voters from overwhelming valid voters when doing voter searches. |
| Denied | The person (citizen or not) was not a registered voter, and their most recent attempt at registration was denied. |
| Incomplete | The citizen is not a registered voter, and their most recent registration attempt was Incomplete. |

| Status | Description |
|----------------|--|
| Pre-registered | The voter has met all the requirements to be an Active voter but has not yet attained the age of 18. Pre-registered voters that will be 18 years old on or before the election date are included in the precinct register and are eligible to vote in the election, even with Pre-registration status. The voter must be 17 years old to pre-register. |
| Pending | As soon as a voter receives a FvrsVoterIdNumber, an entry is made in the FVRS Voter table. For new registrations, prior to HSMV and other match processing, the status of the voter will be Pending. This status is only assigned to people making a new voter registration application which have not yet reached disposition. |

12 VOTER REGISTRATION PROCESSING BY COUNTIES

The following sections describe the typical steps a county voter registration clerk will execute to submit a registration application for a new voter to FVRS. The processes described in the following sections differ slightly from procedures employed for processing applications from HSMV. Such applications will not have a paper application form and will be transmitted electronically to the FVRS.

Further, the procedures described in this section do not include locally defined workflow or processing steps required by counties. Such locally defined steps may include document preparation or scanning of voter registration applications, but will typically not necessitate interface with FVRS.

Further, the steps outlined in this section assume that a voter registration clerk meets all county security requirements for access to the county voter registration system and the county security administrator has granted appropriate FVRS permissions.

12.1 PROCESSING REGISTRATION FORMS FOR VOTERS OUTSIDE OF A COUNTY'S JURISDICTION

FVRS enables any voter registration official to access or update any registration record. This is an important and necessary feature of a statewide system for many reasons including:

- Each voter will be assigned a unique FVRS ID number that will be maintained continuously despite changes in address or voter status. This means that a voter affects a change in legal residence from one county to another through an update to his existing voter registration record. Thus, a voter registration official must be capable of accessing an existing registration record and execute an address update that removes the voter from the jurisdiction of one county and places the voter in another county.

- Any authorized voter registration official shall be capable of simultaneous access to the FVRS from any location with secure communications to FVRS. This offers a previously unavailable level of convenience to the voter for obtaining a common set of services from any voter registration official.
- Voter registration forms may be mistakenly mailed or directed to counties other than the legal residence of a voter. In such cases the jurisdiction receiving the forms shall process the voter registration as described in the sections below and forward the original paper form to the county of jurisdiction. Section 97.053(7) F.S. provides specific direction to voter registration officials under these circumstances.

12.2 GENERAL PROCEDURES

While the following sections relate processing steps by voter registration clerks to transactions serviced by FRS, in fact, the county voter registration system in use will shield the clerk from any direct interface with FVRS transactions. The presentation layer of the county voter registration application shall provide all dialogues and data entry forms to be used by the clerk. The county voter registration system will generate the request to FVRS, receive the FVRS response and format the response message within the presentation layer of county system.

The following sections provide a simplified step-by-step description of typical voter registration processes. Variations in these processes are nearly infinite and may be driven by county standards and procedures.

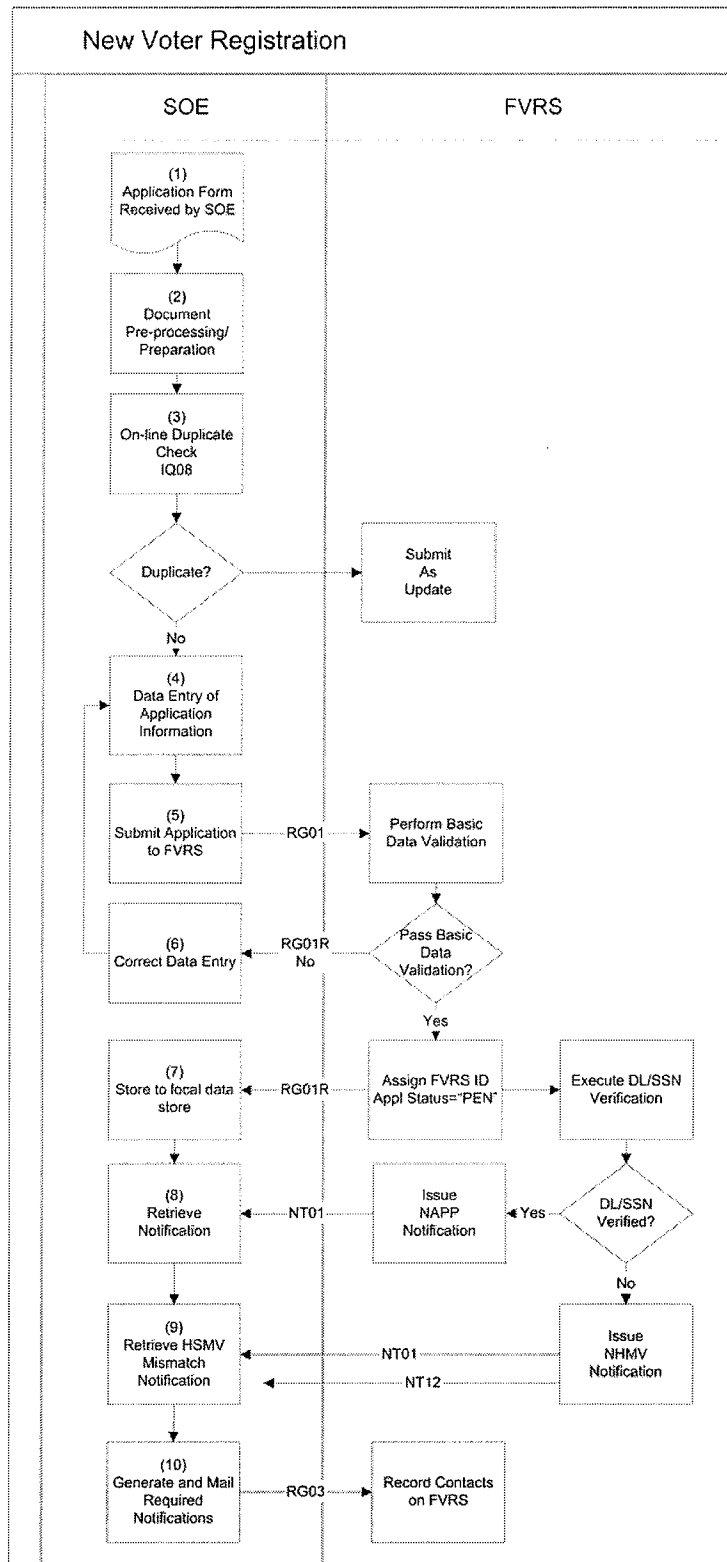
12.3 NEW VOTER REGISTRATION

This section will delineate the key steps involved in processing a new voter registration. Most of the steps comprising the new registration process are depicted in Figure 9.

Steps 1 and 2 – Receipt and Pre-processing Registration Forms

The processing of a new voter registration begins with the receipt of a valid voter registration form. This may be a valid State of Florida voter registration form, a Federal postcard form or a National Mail Registration Form. This step is shown in Figure 9 as step 1. Local procedures for opening mail, time-stamping documents or pre-scanning are not prescribed by FVRS, but are left to the discretion of each county. At a minimum, however, each county should have established procedures for document control and pre-screening for valid documents.

Figure 9 Typical New Voter Registration Process



Step 3 – Check for Possible Duplicate Registration

Before a new voter can be registered with FVRS, a search must be made of the existing registrations on the FVRS data base to insure that the application is indeed a new registration and not an update to an existing one. This is accomplished with the “New Registration” option of the Voter Search transaction (IQ08). Voter identity information such as first name, last name, middle name, and date of birth is submitted to FVRS via the IQ08 input message format. FVRS returns a list of records matching the identity information. Based on the results presented, it is the operator’s decision whether the application represents a new voter registration or an update to an existing registration record. This assessment should be completed for each application regardless of the applicant’s selection of checked boxes on the application form.

While the IQ08 transaction provides for a specific lookup for New Voters as using the name and birth date of the applicant, it also provides for more exhaustive “General” searches based on a variety of criteria such as address, driver’s license number, social security number, etc.

This assessment will become particularly relevant during the critical months after the FVRS becomes operational. During this period most voters may not understand the distinction between a new registration and an update to an existing registration. This may be most evident in a change of address that results in a move between two counties. Prior to FVRS this event would have required the issuance of a new registration, however, after January, 2006 this same action will become an update to an existing registration.

The IQ08 transaction will search both application and voter records (see Section 11). The voter records being searched will include those that are removed (“REM”), administratively (“ADM”) deleted and other voter registration statuses. If the existing voter record has a voter registration status other than “INA”, “ACT”, or “PRE”, then, even though there is an existing record, you should supply the FVRS Voter ID Number but use a TransactionType = ‘R’ for new registration for that record in the RG01 transaction.

An existing *application* can be retrieved using IQ09, and an existing *voter record* can be retrieved using IQ01. County systems can display information from these transactions, to assist with data entry.

Step 4 and 5 – Data Entry of Application and Submission to FVRS

The county’s voter registration program accepts the details from the voter registration form and performs all local data validation edits such as valid dates, compliance with mandatory fields and other minimum data requirements. If the voter resides in the current county, the residence address should be validated against data maintained by the county system and the precinct and district information included in the voter registration details. If the voter resides in a different county, then the FVRS will validate the residential address against the

street and address data maintained in FVRS (see Section 17). The operator may now submit the application to FVRS through the county voter registration system which will invoke an RG01 transaction.

Steps 6 and 7- Edit and FVRS Voter ID Number Assignment

FVRS will reply to an RG01 transaction with an RG01R response. If the application submitted to FVRS cannot be accepted due to basic data validation errors, invalid security or an inability to validate the message digest, the RG01R will respond without assigning an FVRS ID number and with error message(s) enumerating any errors.

If FVRS can accept the applications then the RG01R response will include an FVRS Voter ID Number. The FVRS Voter ID Number will be provided in RG01R only if the RG01 transaction processed successfully. The county voter registration system should display this number to the operator as an acknowledgement and in case local procedures direct this number to be recorded on external documents such as the original registration form. It is also essential that you use this FVRS Voter ID Number in all subsequent transactions concerning the same application.

If no errors are reported in the FVRS RQ01R reply, the processing for steps 6 and 7 are complete and the voter record is given an application processing status of *pending* (see Section 11.1.1).

FVRS will also issue an NAPP notification, providing the county voter registration with an application acknowledgement. An FVRS IQ09 transaction may be used to retrieve the application processing status. Note that a period of time may elapse before the application completes all FVRS verifications and receives an application disposition (see Section 11.1.2).

How to Process Errors Reported by FVRS

FVRS will apply an evaluation immediately to applications submitted through the RG01 transaction. This level of evaluation will be limited to checks for completeness, compliance with basic data format rules, adherence to security and consistency within application elements. Other business rules requiring further verifications against FVRS data or by other external agencies such as Highway Safety (driver's license) or the Social Security Administration (social security number) will be scheduled automatically by FVRS according to processing agreements with those agencies.

Any errors detected by FVRS upon receipt of the application will be reported in the RG01R reply. These error codes should be interpreted and displayed to the operator.

The operator may then correct the data entry and retry the transaction or take one of the following steps to update the application processing status or the

application disposition (see Section 11.1) by processing an RG01 with an appropriate TransactionType.

| Action | Explanation |
|--|--|
| Suspend the Application | The suspended application is held on FVRS with the assigned FVRS Voter ID Number. The application may then be researched, retrieved and completed (see Section 12.7). |
| Update the application disposition as "incomplete" | An NINC notification will be created. Appropriate communications to the voter will be scheduled by FVRS. An NWFL notification is created for an incomplete notice (RegIncomp) (see Section 19) |
| Update the application disposition as "denied" | An NDEN notification will be created. Appropriate communications to the voter will be scheduled by FVRS. |

Scan and Index the Application Image

Final adjudication of an application by the Department may require manual comparison of the voter registration application against other records to ascertain the accuracy of matching processes. This may be particularly true in the felon matching processes to take one example. Access to an image of the voter registration application may, therefore, be necessary to complete the application processing. Thus, the application image should be scanned and transmitted to FVRS within 24 hours of entry of the application into the system.

The FVRS IM01 transaction may be used to transmit document images to FVRS and link them with the appropriate voter record. For each application there may be two images. One is the complete application image, and the other is a clipped signature.

For suspended applications, an NSUS notification is issued to the targeted county after the images have been received by FVRS. For Suspense applications, no further processing is done.

An application that receives a denied or incomplete disposition is fully processed, and only communications with the voter need to be generated.

New applications that are Pending, Denied or Incomplete update the voter's information on the voter table. Suspense applications remain on the application table and do not affect the voter record. For Pending applications proceed to Step 5, otherwise proceed to Step 8.

Step 9 - HSMV Verifies Driver's License Number and/or Last 4 Digits SSN

Only applications with a status of Pending (i.e., step 7 completed without errors) will be forwarded to HSMV for verification of driver's license numbers or last 4 digits of SSN. HSMV will execute verifications of driver's licenses and will determine one of the following:

- Driver's license is correct
- Driver's license number was not provided, but voter appears to have been issued a driver's license
- Driver's license is incorrect or does not match the name provided on the voter registration application

Where necessary HSMV will forward the necessary information to SSA for verification of social security numbers who will provide the following assessment:

- Invalid Data
- Multi Matches All Deceased
- Multi Matches All Alive
- Multi Matches Mixed
- Single Match Alive
- Single Match Deceased
- No Match Found
- System Error: Unable to Process at this Time

The Department will manually review errors and determine if the voter has made an error in reporting their driver's License Number or last 4 digits of the SSN.

- If an error was made, a NHMV notification is created. The county system then uses NT12 to retrieve information about the DL or SSN4 error. If the county determines the voter registration is in error, an RG01 is processed with a transactiontype of 'I'; making the application incomplete. FVRS creates an NINC notification. Proceed to Step 8.
- If the county determines that the registration is correct an RG01 transaction is processed with the HSMVOverride flag set to 'Y'. This progresses the application to Step 6.

FVRS Registration Update

At this point the application is completed and the voter is registered. The voter's status is changed to "ACT".

FVRS creates a Notification to the county SOE for any required communications to the voter. These Notifications typically include pre-registration welcome letters, blank party letters and Voter ID cards. Each document to be sent to the voter will be a notification message.

An NNRG notification is created when a new voter receives an ACT or PRE status. NWFL notifications are created for each of the documents that the voter may receive:

- Blank Party letter
- Pre Registration Letter
- Voter Information Cards

Steps 8 and 9 - County Retrieves Notifications

Notification retrieval is a process execute by the county voter registration system. The purpose of this process is to retrieve notifications from FVRS. Through the notification retrieval process, any changes to the FVRS voter record may be retrieved, and the local database updated. It is only on retrieval of the notification that the county knows whether the new registration attempt has been completed and the disposition assigned to the application and voter registration status.

Step 10 Voter Documents are printed

Contact workflow items are scheduled through the notification process for documents that need to be sent to the voters. When the county prints the documents, a "Registration Contact Add" (RG03) transaction is sent to FVRS.

12.4 UPDATES TO EXISTING VOTER REGISTRATION RECORDS

Step 1 - Search for Existing Voters

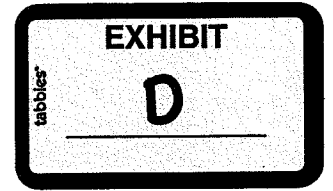
Before an update can be applied to an existing voter registration record, a search must be made of the existing voters. This is accomplished with the FVRS IQ08 transaction. Voter identity information such as voter id number, name, date of birth, etc. is submitted to FVRS via the IQ08 input message format, and FVRS returns a list of records matching the identity information. Based on the results presented, it is the operator's decision whether the application represents a new voter registration or an update to an existing registration record. This assessment should be completed for each application regardless of the applicant's selection of checked boxes on the application form.

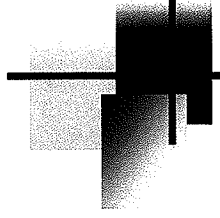
This assessment will become particularly relevant during the critical months after the FVRS becomes operational. During this period most voters may not understand the distinction between a new registration and an update to an existing registration. This may be most evident in a change of address that results in a move between two counties. Prior to FVRS this event would have required the issuance of a new registration, however, after January, 2006 this same action will become an update to an existing registration.

The IQ08 transaction will search all voter records (see Section 11). The voter records being searched will include those that are removed ("REM"), archived ("ADM") deleted, Pending ("PEN") and other voter registration statuses. If you are able to locate an existing record for the person being processed, you should supply the FVRS Voter ID Number for that record in the RG01 transaction.

SSA's HAVA Verification

Peter Monaghan
Social Security Administration
February 6, 2006





Legislation Verification Highlights

- MVA responsible for verifying information and working with SSA
- Drivers License number primary source
- If no DL/ID, election agency collects last four digits of SSN
- SSA must develop process to provide “last four digit” verification
- SSA to be reimbursed for funds expended

System Development

Highlights

- October 2002 – President signs HAVA
- November 2002 – SSA begins internal work
- February 2003 – SSA & AAMVA reach conceptual agreement on telecommunications
- May 2003 – SSA joins NASS-NASED-AAMVA Task Force
- January 2004 – “Joint Communiqué” sent to MVAs, Election Agencies
- August 2004 – SSA’s systems development complete
- October 2004 – First live use of system (Iowa)



Agreements

- Election Agency - MVA
- MVA - AAMVA
- AAMVA - SSA: telecommunications and billing
- SSA & MVA: Privacy, process and reimbursement



SSA/MVA Agreement Process

- SSA developed “model” agreement
- Discussions between SSA Regional Office and MVA
- “Final” agreement reviewed by SSA attorneys
- Signed by MVA and Regional Commissioner
- Data transmission can begin



Participation to Date

55 total jurisdictions:

- 8 exempt
- 23 signed agreements
 - 19 implemented
 - 4 in testing
- 8 final review of agreement
- 13 agreements underway
- 3 no current SSA activity



Implementation Process

- Agreement discussions SSA/MVA
- Systems testing with “dummy” data
- Agreement finalized
- Exchange of “live” data can begin



Verification Routine

- Election agency collects name, DOB and last four digits of SSN
- Transmitted to MVA
- MVA transmits to SSA via AAMVA
- SSA does exact search of name, month/year of birth and “last four”
- Real-time reply sent to MVA via AAMVA

Verification Replies

| Response Code | Definition |
|----------------------|----------------------------|
| S | Invalid Data |
| T | Multi Matches All Deceased |
| V | Multi Matches All Alive |
| W | Multi Matches Mixed |
| X | Single Match Alive |
| Y | Single Match Deceased |
| Z | No Match Found |
| 9 | System Error |

Results to Date


143,000 queries

| Response | Percent |
|----------------------------|----------------|
| Invalid Data | .001% |
| Multi Matches All Deceased | 0 |
| Multi Matches All Alive | .014% |
| Multi Matches Mixed | .001% |
| Single Match Alive | 69% |
| Single Match Deceased | 2.5% |
| No Match Found | 28.5% |



Reimbursement

- SSA legally precluded from using trust funds for non-SSA work
- HAVA specifically provided for reimbursement
- Development, maintenance and ongoing SSA & AAMVA costs included
- Billing through AAMVA



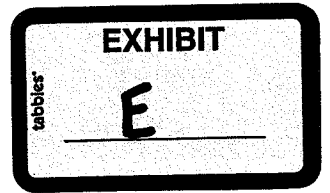
Contact Information

Pete Monaghan:

- 410-966-9972
- Pete.Monaghan@SSA.gov

SSA's HAVA Verification

Peter Monaghan
Social Security Administration
February 12, 2007





Participation to Date

55 total jurisdictions:

- 7 exempt
- 42 signed agreements
 - 32 implemented
 - 10 in testing or not yet using
- 3 agreements underway
- 3 other



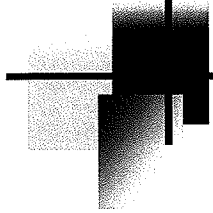
Agreements

- Election Agency - MVA
- MVA - AAMVA
- AAMVA - SSA: telecommunications and billing
- SSA & MVA: Privacy, process and reimbursement



Reimbursement

- SSA legally precluded from using trust funds for non-SSA work
- HAVA specifically provided for reimbursement
- Development, maintenance and ongoing SSA & AAMVA costs included
- Billing through AAMVA



Development Highlights

- NASS sponsored workgroup:
 - NASED, AAMVA, SSA, several States
- Desired outcomes:
 - Prevent fraudulent voting
 - Avoid incorrect prevention of registration
 - Provide maximum information
- Group developed requirements based on:
 - Desired outcomes
 - Limitations of information



Design Considerations

- Limited input information
- Balance inclusion v. exclusion
- True match unknowable:
 - Each “last four” equals 40,000 SSNs
- Provide maximum output information to election agency

Verification Routine

- Election agency collects name, DOB and last four digits of SSN
- Transmitted to MVA
- MVA transmits to SSA via AAMVA
- SSA does exact search of name, month/year of birth and “last four”
- Real-time reply sent to MVA via AAMVA

Verification Replies

| Response Code | Definition |
|----------------------|----------------------------|
| S | Invalid Data |
| T | Multi Matches All Deceased |
| V | Multi Matches All Alive |
| W | Multi Matches Mixed |
| X | Single Match Alive |
| Y | Single Match Deceased |
| Z | No Match Found |
| 9 | System Error |

Results to Date

2.6 million queries

| Response | Percent |
|-------------------------|----------------|
| Single Match - Alive | 53.3% |
| Single Match - Deceased | .3% |
| No Match Found | 46.2% |
| All Other | .3% |



Results

- False positives cannot be identified
- Match rate?
 - Last name changes not reported to SSA
 - Proper first name historically not required
 - Exact month/year of birth required
- SSA data may be outdated, incorrect



Contact Information

Pete Monaghan:

- 410-966-9972
- Pete.Monaghan@SSA.gov

9/27/2004

**BOARD OF ELECTION & DEPARTMENT OF MOTOR VEHICLE
IDENTIFICATION VERIFICATION REPORT**

| BOROUGH | BOE DATA ENTRY ERROR | VOTER ERROR | DMV ? | TOTAL PER BORO |
|-----------------------------|---------------------------------|------------------------|------------------|---------------------------|
| MANHATTAN | 1009 | 228 | | 1237 |
| BROOKLYN | 885 | 171 | 2 | 1058 |
| QUEENS | 670 | 140 | 5 | 815 |
| BRONX | 250 | 48 | | 298 |
| STATEN ISLAND | 137 | 22 | 1 | 160 |
| TOTAL COUNTYWIDE | 2951 | 609 | 8 | 3568 |

BOE Data Entry Errors – Numbers were data entered wrong.

Social Security numbers were put in as the drivers I.D. #.

Telephone numbers were put in as the drivers I.D. #.

Voter serial numbers were put in as the drivers I.D. #.

Zip code numbers were put in as the drivers I.D. #.

Voter Errors - Social Security numbers were put in as the drivers I.D. #.

Out of state driver I.D. # (only the number, not a copy of their card).

Number did not match DMV I.D. # .

DMV Errors – Voter on Queens DMV list, but moved to Staten Island.

DMV I.D. # matched the DMV voter registration, same name, same date of birth, but on DMV Error Report.

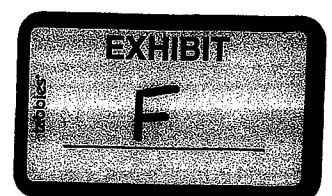


EXHIBIT G

FLORIDA VOTER REGISTRATION APPLICATION

YOU CAN USE THIS FORM TO: REGISTER TO VOTE IN THE STATE OF FLORIDA • CHANGE NAME OR ADDRESS • REPLACE YOUR DEFACED, LOST, OR STOLEN VOTER INFORMATION CARD • REGISTER WITH A POLITICAL PARTY OR CHANGE PARTY AFFILIATION • UPDATE YOUR SIGNATURE

To Register, You Must:

- Be a citizen of the United States of America. (BOX #2)
- Be a Florida resident. (BOX #8)
- Be 18 years old (you may pre-register if you are 17). (BOX #5)
- Not now be adjudicated mentally incapacitated with respect to voting in Florida or any other state. (BOX #4)
- Not have been convicted of a felony in Florida, or any other state, without your civil rights having been restored. (BOX #3)
- Provide your current and valid Florida driver's license number or Florida identification card number. If you do not have a current and valid Florida driver's license or Florida identification card, you must provide the last four digits of your Social Security number. If you do not have a FL DL#, FL ID card#, or SSN, write "NONE" in the box. (BOX #6)
- Complete all information in the black boxes on the application. (BOXES #2,3,4,5,6,7,8 & 16)

Deadline Information:

If this is a new registration application, the date the completed application is postmarked or hand delivered to a driver's license office, a voter registration agency, an armed forces recruitment office, the Division of Elections, or the office of any supervisor of elections in the state will be your registration date. If this is a new Florida application, you must be registered for at least 29 days before you can vote in an election. If your application is complete and you are qualified as a voter, a voter information card will be mailed to you.

Party Affiliation (BOX #12):

If you wish to register with a major political party, place an "X" in the box preceding the listed party with which you wish to affiliate. If you wish to register with a minor political party, place

an "X" in the box preceding "Other, Minor Party" and print the name of the party with which you wish to affiliate. A list of the minor political parties is on the website for the Division of Elections: <http://election.dos.state.fl.us/online/parties.shtml> If you wish to register without party affiliation, place an "X" in the box preceding "No Party Affiliation".

Florida is a closed primary state. If you wish to register to vote in a partisan primary election, you must be a registered voter in the party for which the primary is being held. All registered voters, regardless of party affiliation, can vote on issues and non-partisan candidates.

Notice:

The office at which you register, or your decision not to register, your SSN, your FL DL# and

your FL ID card# will remain confidential and will be used only for voter registration purposes.

Note: If the information on this application is not true, the applicant can be convicted of a felony of the third degree and fined up to \$5,000 and/or imprisoned for up to five years.

Questions:

Contact the office of your county supervisor of elections for additional information. Contact information is on the website for the Division of Elections: <http://election.dos.state.fl.us/county/index.shtml>

Informacion en Espanol:

Sirvase llamar a la oficina del supervisor de elecciones de su condado si le interesa obtener este formulario en Español.

PLEASE COMPLETE THE APPLICATION BELOW. PLEASE PRINT USING A BLACK BALL POINT PEN.

- 1) Black boxes must be completed on the application below for registration to be valid.
- 2) Return this completed application to the office of your supervisor of elections.
- 3) If you are a first-time voter in this state applying by mail to register to vote and you have not been issued a FL DL#, FL ID#, or SSN, include a copy of your ID with the application.
- 4) Mail with first class stamp.

FLORIDA VOTER REGISTRATION APPLICATION

REVISED 1/06

| | | | | | | | | | | | |
|----------|---|--|--|--|--------------------------------------|------|---|-------------------------------------|---------------------------|---|--|
| REQUIRED | 1 | Check boxes that apply: <input type="checkbox"/> New Registration <input type="checkbox"/> Address Change <input type="checkbox"/> Party Change <input type="checkbox"/> Name Change <input type="checkbox"/> Card Replacement <input type="checkbox"/> Signature Update | | | | | | OFFICIAL USE ONLY: DS DE 39 1/06 | | | |
| | 2 | Are you a citizen of the United States of America? Yes? <input type="checkbox"/> No? <input type="checkbox"/> (if NO, you cannot register to vote) | | | | | | | | | |
| | 3 | <input type="checkbox"/> I affirm I am not a convicted felon, or if I am, my rights relating to voting have been restored. | | | | | | | | | |
| | 4 | <input type="checkbox"/> I affirm I have not been adjudicated mentally incapacitated with respect to voting or, if I have, my competency has been restored. | | | | | | | | | |
| | IF YOU ANSWERED NO TO QUESTION 2, OR IF YOU ARE UNABLE TO AFFIRM THE STATEMENTS IN BOXES 3 AND 4, YOU ARE INELIGIBLE TO REGISTER TO VOTE. DO NOT COMPLETE THIS APPLICATION. | | | | | | | | | | |
| | 5 | Date of Birth (MM/DD/YYYY) | | / / | | | | | | | |
| | 6 | If you have a current and valid FL DL# or FL ID card#, you must provide the number in this box. If you do not have either, provide the last 4 digits of your SSN. If you have not been issued a FL DL#, FL ID card#, or SSN, write "NONE": | | | | | | | | | |
| | 7 | Last Name | | | Suffix (circle) Jr. Sr. II III IV | | First Name | | Middle Name/Initial | | |
| | 8 | Address Where You Live (Legal Residence) DO NOT GIVE P.O. BOX | | | Apt/Lot/Unit | City | County of Legal Residence | | State | Zip Code | |
| | 9 | Mailing Address If Different from Above | | | Apt/Lot/Unit | City | Country | | State | Zip Code | |
| | 10 | Address Last Registered to Vote | | | Apt/Lot/Unit | City | County | | State | Zip Code | |
| | 11 | Former Name if Making Name Change | | | | | Day Phone Number | | | | |
| | 12 | Party Affiliation (Check only one) <input type="checkbox"/> Democratic Party <input type="checkbox"/> Republican Party <input type="checkbox"/> Other, Minor Party (print party name): | | | | | | | | <input type="checkbox"/> No Party Affiliation | |
| | 13 | Race/Ethnicity (Check only one) <input type="checkbox"/> American Indian/Alaskan Native <input type="checkbox"/> Asian/Pacific Islander <input type="checkbox"/> Black, not Hispanic <input type="checkbox"/> Hispanic <input type="checkbox"/> White, not Hispanic | | | | | | | | | |
| | 14 | Sex <input type="checkbox"/> M <input type="checkbox"/> F | | Do you need voting assistance at the polls? <input type="checkbox"/> Yes <input type="checkbox"/> No | | | Are you interested in being a poll worker? <input type="checkbox"/> Yes <input type="checkbox"/> No | | State or Country of Birth | | |
| 15 | Are You: <input type="checkbox"/> Active Duty Military/Merchant Marine <input type="checkbox"/> Dependent of Active Duty Military/Merchant Marine <input type="checkbox"/> U.S. Citizen Currently Residing Outside the U.S. | | | | | | | | | | |
| REQUIRED | 16 | OATH: I do solemnly swear (or affirm) that I will protect and defend the Constitution of the United States and the Constitution of the State of Florida, that I am qualified to register as an elector under the Constitution and laws of the State of Florida, and that all information provided in this application is true. | | | | | | | | | |
| | SIGNATURE: Sign or mark on line in box below. (Invalid without signature or mark of applicant.) | | | | | | | | Date: | | |
| X | | | | | | | | | | | |

SPECIAL IDENTIFICATION REQUIREMENTS

If you are registering by mail, you have never voted in Florida, and you have not been issued a Florida driver's license, Florida identification card, or Social Security number, you will be required to provide additional identification prior to voting the first time. To ensure that you will not have problems when you go to vote, you should provide a copy of the required identification listed below at the time you mail your voter registration application.

You may provide a copy of one of the following photo identifications (ID) that includes your name and picture:

- U.S. Passport
- Employee Badge or ID
- Buyers Club ID
- Debit/Credit Card
- Military ID
- Student ID
- Retirement Center ID
- Neighborhood Association ID
- Public Assistance ID

Or, you may provide a copy of one of the following documents that contains your name and current residence address:

- Utility Bill
- Bank Statement
- Government Check
- Paycheck
- Other Government Document

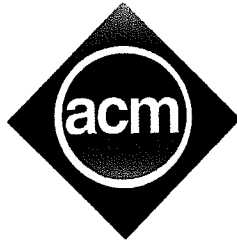
Or, if you are one of the following persons, you are exempt from having to provide a copy of an ID at this time.

These exemptions are:

- Persons 65 years of age or older
- Persons with a temporary or permanent physical disability
- Members of the active uniformed service or merchant marine who, by reason of such active duty, are absent from the county
 - Spouse or dependent of an active uniformed service member or merchant marine who, by reason of the active duty or service of the member, is absent from the county
 - Persons currently residing outside the U.S. who are eligible to vote in Florida

**All voters are required to provide ID containing photo and signature at the time of voting in the polling place.
Without proper identification, a voter can only vote a provisional ballot.**

DO NOT SEND ORIGINAL IDENTIFICATION DOCUMENTS TO THE SUPERVISOR OF ELECTIONS.

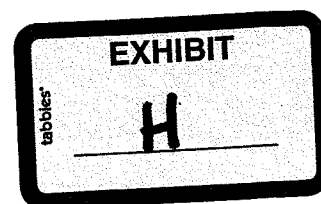


Association for Computing Machinery
Advancing Computing as a Science & Profession

Statewide Databases of Registered Voters:
Study Of Accuracy, Privacy, Usability, Security, and Reliability Issues commissioned by
the U.S. Public Policy Committee of the Association for Computing Machinery

February 2006

Copyright © 2006 ACM [X]. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.



Preface

The Association for Computing Machinery (ACM) is an educational and scientific society uniting the world's computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. As such, ACM cares deeply about the dependability and reliability of computing technology. Voter registration systems encompass not only the databases that house voter information, but also an entire information technology infrastructure that must be carefully managed by election officials. The U.S. Public Policy Committee of the ACM (USACM) commissioned this study to provide objective technical information and expert recommendations to state and local election officials, policy makers, and the public about these systems.

The USACM serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology.

Supported by ACM's Washington, D.C., Office of Public Policy, USACM responds to requests for information and technical expertise from U.S. government agencies and departments, seeks to influence relevant U.S. government policies on behalf of the computing community and the public, and provides information to ACM on relevant U.S. government activities. USACM also identifies potentially significant technical and public policy issues and brings them to the attention of ACM and the public.

More information about ACM may be found on the World Wide Web at <http://www.acm.org>, and information on USACM may be found at <http://www.acm.org/usacm>.

Table of Contents

| | |
|---|----|
| Executive Summary | 4 |
| Chapter Overviews and Recommendations..... | 8 |
| 1. Introduction..... | 17 |
| 2. Accuracy..... | 21 |
| 3. Privacy..... | 27 |
| 4. Usability..... | 33 |
| 5. Security..... | 39 |
| 6. Reliability | 50 |
| Appendix A: Glossary..... | 54 |
| Appendix B: Biographies of Committee Members..... | 57 |

"An adequate and effective registration will go far toward assuring honesty and fairness in the conduct of elections. Upon the honest and faithful maintenance of the registration books depends the purity of the ballot box. And upon the purity of the ballot box depends the success or failure of our democratic form of government."

-- *Registration of Voters in Louisiana*, Alden L. Powell and Emmett Asseff, Bureau of Government Research, Louisiana State University, 1951

Executive Summary

The voter registration process may seem simple to most voters. They give their names, addresses, birth date, and in some cases party affiliations to election officials with the expectation that they will be able to vote on Election Day. In reality, election officials must oversee a complex system managing this process. They must ensure that the voters' information is accurately recorded and maintained, that the system is transparent while voter information is kept private and secure from unauthorized access, and that poll workers can access this information on Election Day to determine whether or not any given voter is eligible. A well-managed voter registration system is vital for ensuring public confidence in elections.

State and local governments have managed voter registration using different approaches among different jurisdictions. In 2002, Congress sought to make these disparate efforts more uniform by passing the Help America Vote Act, which required that each state have a computerized statewide voter registration database. In implementing this mandate, state and local governments still have differing approaches, but it is clear that information technology underpins each of their efforts. While technology will help election officials manage this complex system, it also creates new risks that must be addressed.

This study focuses on five areas that election officials should address when creating statewide voter registration databases (VRDs): accuracy, privacy, usability, security, and reliability. Each chapter contains detailed discussions and recommendations. The following are some of the overarching goals for VRDs and selected recommendations for achieving them.

1. The policies and practices of entire voting registration systems, including those that govern VRDs, should be transparent both internally and externally.

VRDs control access to voting; therefore, they have a direct impact on the fairness of elections, as well as the public's perception of fairness. It must be possible to convince voters, political parties, politicians, academics, the press, and others that VRDs are correct and are operating appropriately. Internal procedures and interfaces also must be clear to election workers in order to minimize errors. Transparency can be provided by allowing voters to verify their voter registration status and data; publicly disclosing outside data sources that officials use for verification; indefinitely keeping a secure write-