FRANK ASKIN, Esq.
PENNY M. VENETIS, Esq.
Rutgers Constitutional Litigation Clinic
123 Washington Street
Newark, New Jersey 07102
(973) 353-5687
Attorneys for Plaintiffs

Assemblyman Reed Gusciora, Stephanie G. Harris, Coalition for Peace Action, and New Jersey Peace Action, Plaintiffs, v. James E. McGreevey, Governor of the State of New Jersey (in his official capacity), and Peter C. Harvey, Attorney General of the State of New Jersey (in his official capacity), Defendants.	SUPERIOR COURT LAW DIVISION MERCER COUNTY Docket No. CIVIL ACTION **CERTIFICATION OF REBECCA MERCURI**

Rebecca Mercuri, being of full age, hereby certifies:

Credentials

1. I currently hold a fellowship at the Radcliffe Institute for Advanced Study at Harvard University and receive some additional support from a fund at Harvard's John F. Kennedy School of Government. I received a Ph.D. from the University of Pennsylvania's School of Engineering

and Applied Sciences, where I wrote a dissertation that was defended in October 2000 entitled "Electronic Vote Tabulation: Checks & Balances." I also hold a Master of Science in Engineering from the University of Pennsylvania, a Master of Science in Computer Science from Drexel University and a Bachelor of Science in Computer Science from the Pennsylvania State University.

2. My primary fields of expertise are computer security and real-time interactive computer systems (which would encompass those used for voting). I author the "Security Watch" column for the Communications of the Association of Computing Machinery and have written over two dozen technical papers on various computer and election-related topics. A copy of my curriculum vitae is attached hereto as Exhibit A.

3. I have been employed as a computer expert witness by the NJ Office of the Public Defender, the NJ Office of Attorney Ethics, and various law firms, in a number of civil and criminal cases in the State of New Jersey.

4. I have provided expert testimony in the US and UK on the subject of electronic voting since the early

1990's. I have provided testimony for cases in California and Florida, including the Bush v. Gore dispute; have appeared before various municipal boards and state legislative bodies; and have prepared formal statements and interrogatories for federal agencies, including: the US House Science Committee, the US Commission on Civil Rights, the Federal Election Commission, and the UK Cabinet's Office of the E-Envoy. All of my expert testimony work on voting issues, including this case, has been pro bono, although occasionally I have received some expense remuneration.

5. I am also an active member of the Institute of Electrical and Electronics Engineers' working group that is preparing a voting system standard that is expected to be delivered to the US Election Assistance Commission in the early part of 2005.

Background

6. All of the statements that I have provided in this certification are based on my research since 1989 on the subject of electronic voting. I conducted my research by reading scientific literature, reviewing information

about election systems that is in the public domain, analyzing election result data, reading news reports from bona-fide sources (such as the New York Times and the Washington Post), discussing electronic voting technology with vendors and election officials, attending conferences and hearings, and participating in walk-through inspections of equipment.

7. Although I have been prevented from performing an end-to-end evaluation of any electronic voting systems due to the trade secrecy practices that have been imposed by the manufacturers, the information I have gathered in the aforementioned ways has enabled me to assert various facts about the election systems in question in this case.

Flaws with Electronic Voting Systems

8. Lack of provability.

It is currently impossible to determine that a computational system is performing only a certain set of tasks and no more.

a) All fully-electronic voting systems suffer from this problem. This flaw results from the fact that it is impossible to prove that no nefarious or incorrect code

exists within a system, regardless of how thorough an inspection of its hardware and software may appear to be.

b) This lack of provability is currently unsolvable by computer science theory. One effect of this unsolvable problem allows the insertion of rogue instructions that can provide undetectable alteration of the internal programming of a computer system such that it no longer reflects the intentions of the original source code. Such a nefarious program in an election system may even be able to delete itself along with the traces of its existence during the shut-down procedure at the end of the voting session.

c) The impact of this fundamental flaw on voting systems means that no matter how stringent the testing and certification may be, this can not guarantee that the system will be 100% secure and 100% reliable.

Electronic Voting Machines Have Malfunctioned In Ways That Disenfranchise Voters.

9. Despite manufacturer claims to the contrary, electronic voting systems are not fail-safe.

a) In 2000, newly purchased Sequoia Voting Systems AVC Advantage ballot casting devices in South Brunswick, New

Jersey failed to shut down or issue an alert when an internal malfunction occurred, causing zero votes to be reported for certain major-party candidates.

b) I have a copy of a videotape that was made in 1995 in Jefferson Parish, Louisiana, showing a post-election test that demonstrated Sequoia Voting Systems voting machines occasionally displaying the incorrect candidate's name on the LCD (liquid crystal display) panel when the button for a candidate, adjacent to the one whose name was shown, was pressed. It was never resolved whether the votes were also attributed to the incorrect candidate.

10. As electronic voting systems have been deployed in increasing numbers throughout the US, there have been an increasing number of reports of malfunctions resulting in the deletion and/or shifting of votes.

11. Since DRE voting system equipment is protected by trade secrecy from thorough review, it is not possible to determine whether the problems have resulted from inadvertent software, hardware or data errors, or malicious manipulation.

12. Regardless of the cause of these malfunctions, when such problems do occur, it is impossible to

reconstruct the intention of the voters, because the ballot data that has been recorded will, in many cases, also reflect the problem that had ensued.

13. Other equipment malfunctions, such as battery charging errors or start-up problems (as have occurred in CA and FL), can cause a shutdown of the voting system. When extensive, the emergency paper ballot supply for a precinct or county has been depleted, resulting in voters being turned away at the polls.

Electronic Voting Systems Are Less Accurate Than Other Forms of Voting.

14. Various analyses of election data have revealed that fully-electronic voting systems have a poorer "residual" vote rate (a calculation of the percentage of votes not recorded for an election as compared to the total number of voters who had cast ballots) than optically scanned paper balloting systems (the most commonly used voting system in the US). For example, a study conducted earlier this year by the Florida Sun Sentinel showed electronic voting to have a residual vote rate 6 times larger than optically scanned ballots. In close elections,

these "missing" votes can certainly affect the outcome of a race if they were not intentional. David Cho and Lisa Rein, Fairfax to Probe Voting Machines, The Washington Post, November, 18, 2003.[1]

15. Since it is not possible to determine the cause of the missing votes, and since fully electronic systems do not provide any way to perform an independent recount of the ballots, voters using the electronic machines may be unfairly and unequally disenfranchised.

16. With optically scanned systems, a manual audit of the paper ballots can reveal computer malfunctions. Examples of such malfunctions that were detected include: the misprogramming of Democratic ballots in a primary election in Florida so that they were all recorded for Republican candidates, and a calibration flaw with some scanners in California that caused them to view ballots prepared with gel ink pens as being blank.

Electronic Voting Machines Are Vulnerable To Insider Attacks.

17. With regard to security, electronic voting

[1] Available At http://www.washingtonpost.com/wp-dyn/articles/A54432-

systems are vulnerable to insider attacks as well as those from outside "hackers," although the insider attacks are considerably more possible. In the spring of 2004, I had the opportunity to observe the election setup procedures used for the Sequoia Voting Systems AVC Advantage systems in Montgomery County, PA. The equipment supervisor demonstrated how the ballot programming in the cartridge could be replaced using the keypad on the side of the voting machine or through transfer (downloading) from another cartridge. This was explained to be a "feature" that could be used in case a cartridge was found to be defective. In fact, what this feature provides is an opportunity for election workers and also vendor staff (who are often on site) to change how the names of candidates are correlated with those printed on the paper that covers the button panel.

18. There are a number of such avenues for such types of circumvention, and some machines (including the Sequoia Voting Systems AVC Edge model) allow for complete reprogramming of the entire device through a slot on the front of the machine that is protected only by a small plastic tab following election setup.

19. Although the vendors claim that such reprogramming would be detected during the post-election audit, since this audit is performed by the same insiders who set up the machines, it would certainly be possible for them to cover up any nefarious intent.

20. The auditing software for electronic voting systems has been found to be flawed and highly insecure, especially some products supplied by ES&S and Diebold. Those two vendors were also discovered during 2003 and 2004 to have substituted uncertified software into machines that were subsequently used in elections in CA, IN, FL, MD and GA, despite the fact that such substitution constituted a violation of state election laws.

DRE Voting Systems Are Not Transparent, Making It Impossible to Detect Tampering Activities.

21. Many DRE voting systems contain an external button which allow the machines to be reset. In the Sequoia Voting Systems AVC Advantage, a button on the back of the machine allows the machine to be locked after a vote is cast (so that a voter cannot vote multiple times) and to set the machine for the next voter. In lever machines this

locking was noticeable (the curtain would open noisily, and the poll worker had to pull out a long button that was visible to everyone in the polling station). In my observations of the Sequoia Voting Systems AVC Advantage systems I have not noticed such an overt alert when the button on the outside of the machine is pressed. Though this button was intended as a security feature, a poll worker could potentially conspire with a voter to manipulate the election by depressing the exterior button multiple times, allowing someone inside of the booth to cast additional votes. Although these extra votes might be noticed in the end of day comparisons to the voter totals from the sign-in book, there would be no way to differentiate the illegal votes from the actual ones, so this could be used to invalidate that machine's votes. As a poll worker in New Jersey, I once witnessed an incident involving a fleeing voter (one who started but did not complete the voting process) that placed a machine's results into question – in that case, since it was a lever machine, all of the poll workers could attest to what had been observed. This might not have been possible if a DRE had been used, thus all voters who had used the

disqualified machine could be disenfranchised.

22. Certain buttons on the outside of the Sequoia Voting Systems AVC Edge machines also may pose vulnerability issues. It is my understanding that one button on the back can be pushed to shift the machine into supervisor mode. This button is used by poll workers to perform administrative functions. As described above, this button could be used to manipulate elections. I have a copy of a videotape showing the use of this button to perform a resetting function where it was unclear whether a ballot was subsequently cast or just voided. Another button on the outside of the AVC Edge is used to shut down the machine. With the lever machines there were two keys in a hard-to-reach (and visible) place on the top of the machine that poll workers had to turn in order to close the machines from vote casting and allow the reading of vote totals at the end of the election day. This relatively easy-to-access button on the AVC Edge, like any other active button or port on the outside of a DRE voting system, presents a vulnerability and invites tampering with the election.

Vendors Have Not Acted Responsibly When There Have Been Software Flaws.

23. Vendors have not generally been forthcoming in disclosing flaws in their machines or in providing recalls when software and equipment has been determined to be flawed. There is no national or state repository where problem reports can be checked, leaving communities to fend for themselves in attempting to determine if their voting systems may be at risk.

24. The procurement agreements for voting equipment often require hefty licensing fees and service contracts, so local election officials are bound to the vendors following their purchases. Here again, since election officials are not privy to the details pertaining to the inner workings of the machines (supposedly for security reasons, although the discussion here certainly indicates that security can be breached), they have no way to know if the equipment is in fact running the appropriate versions of the software, or if a vendor representative has done something to any of the machines through its programming portal that could change its operations.

25. In the case of the Sequoia Voting Systems AVC

Advantage, the claim has been made by the vendor that since the ballot cartridges contain only data, there is no way to alter the fundamental operations of the machine through that channel. In actual fact, though, this vendor admitted in hearings in the mid-1990's in New York City (where I was testifying on the procurement contract which was ultimately abandoned) in response to my query, that it is certainly possible for the Z80 microprocessor used by the AVC Advantage to interpret data as programming (object code) and vice versa. There are other internal features of the Z80 processor (such as its swap registers) that can be exploited to take advantage of and conceal inappropriate internal configurations.

26. To a microprocessor, there is basically no difference between the binary codes that represent data and those that represent programs. It is therefore quite simple to write a program that branches into a data segment and then begins executing it as code. If this occurs, then any programming commands could be inserted, such as those that swap or incorrectly tally votes. The Sequoia Voting Systems representatives at that NYC hearing did not provide any assurances that could be used to determine whether or

not this could occur, nor did they indicate that they had applied any remediation to the system in order to ensure that it would not occur. So the claim that the cartridge contains only "data" may be a smokescreen. Having programmed with the Z80 for a number of years in industry, I believe that voting machines that still use this microprocessor (like the Sequoia AVC Advantage) are highly vulnerable to this flaw. Later microprocessors (like the Intel Pentium) were designed with additional safeguards to prevent this exploit from occurring.

Inadequate Certification Procedures.

27. The voting machine certification process described in New Jersey statutes is not necessarily one that will assure the proper functioning and security of DRE voting systems. For example, it is unclear whether the certification committee, as presently composed, has the appropriate quality assurance and computer security skills needed to evaluate the accuracy, integrity, reliability, and auditability of DRE voting systems.

28. Only certification procedures that use "white box" evaluation (a process which thoroughly examines all

hardware and software, including source code), along with "black box" tests (on the functionality of the machine under each of the possible permutations which may occur in an election scenario), can be considered comprehensive. The limited "black box" testing prescribed by the NJ statute is insufficient to flush out all of the problems with a DRE voting system. The testing performed by the certification committee is certainly not comprehensive, as that would require a considerably larger staff and thousands of hours to perform.

29. The policies and procedures used in certifying DRE voting machines must be made available to the public for review in order to assure that they are comprehensive and adequate. The policies and procedures used by election workers during elections using DRE voting machines must also be made available to the public for inspection in order to determine their adequacy and efficacy.

30. Software changes that will affect the function of DRE voting systems should prompt recertification procedures. Presently, there is no procedure whereby voting systems are decertified. Minimally, any substantive change of software should revoke certification, and all

software should be retested, as changes in one area of the programming can affect the operations of other code segments. The Election Assistance Commission has recommended the use of configuration management tools that provide assurances that the software modules (object code) inside of the voting systems are identical to those that have been certified. It is unlikely that New Jersey has implemented such controls or that they have plans to do so for the November 2004 or subsequent elections.

31. The certification of only a small percentage of voting machines is inadequate. Each machine could possess unique flaws in its hardware (such as wiring problems) that could cause it to malfunction. In addition, the software installed on each machine may not be identical. The State of Georgia has shown that inspection of only a small percentage of voting machines does not identify all defective machines. Georgia has implemented a program whereby every individual voting device is tested prior to being deployed for use. They have rejected hundreds of machines that were inappropriately configured by the manufacturers or were deemed defective. Implementing Voting Systems: The Georgia Method, Communications of the

Association for Computing Machinery, October 2004.

32. Because testing cannot determine all flaws, including some flaws that could affect the recording and tallying of votes, there must be procedures in place to check tabulation results against the true intent of voters, such as by using a voter-verified paper ballot (as described below).

33. The inspections that are currently being performed on voting systems are flawed in ways beyond the inadequacies noted above. For example, it has not been well publicized that all electronic voting systems purchased through 2003 (and some also in 2004) were certified only to the Federal Election Commission's 1990 guidelines, deemed obsolete by the FEC in the late 1990's. Voting equipment is grandfathered and is not required to be updated, even if security or reliability flaws later become evident. The FEC replaced their 1990 guidelines in 2002, but this new set of examination criteria was also deemed flawed, especially in the areas of usability and security. The FEC Proposed Voting Systems Standard Update: A Detailed Comment by Dr. Rebecca Mercuri, September 10, 2001.[2] In particular,

[2]Available At www.notablesoftware.com/Papers/FECRM.html

the 1990 and 2002 guidelines provided a blanket exemption from inspection for COTS (Commercial Off The Shelf) products that are incorporated into or used to develop voting systems, despite the fact such components (like Microsoft operating systems and compilers) are well known to provide avenues for security breaches.

34. The Institute of Electrical and Electronics Engineers has been working for the past three years on a more rigorous standard that would eliminate many of these overt loopholes, but systems designed to the IEEE specifications will not appear until 2006 (at the earliest). What is known as the "federal" certification testing is actually a process performed by "independent testing authorities" (ITAs) who can hardly be called independent, since testing is paid for by the vendors and the details of the tests are protected from disclosure by trade secrecy agreements. It is not apparent whether or not New Jersey subscribes to this process by requiring all of their voting systems to have ITA certification, although currently the systems in use do have this approval. So, it must be assumed that unless the State of New Jersey performs additional testing to mitigate the flaws of the

ITA process, these loopholes also exist in New Jersey's election equipment.

Lack Of Independent Audit - The Need For Voter-Verified Paper Ballots.

35. Even inexperienced programmers are capable of writing software that accepts some input and displays seemingly appropriate output on a computer screen, while recording something else and subsequently printing out an "audit trail" that is consistent with the misrecorded information. This is certainly possible with a voting system.

36. Fully-electronic voting systems do not provide any independent way to validate that the ballots cast have accurately transcribed the intentions of the voters, nor that the vote totals have been properly computed. Optically scanned voting systems do not have these problems because the voter transcribes their intentions directly onto a paper ballot, and these paper ballots are available for recount purposes if the computer tallying systems are later questioned.

37. Vendors of DRE systems have supplied an option

whereby the entire set of electronically recorded ballot images may be printed out at the end of the election, but since the voters do not have any opportunity to verify that these after-the-fact printed ballots correctly convey their votes (due to the anonymity requirement), such self-audits are moot.

38. In response to the growing outcry for voter-verified paper ballots with the electronic systems, Sequoia Voting Systems has supplied units to the state of Nevada that do print paper ballots for voter review at the polling station. The problem with these systems is that they were designed such that the paper is on a continuous roll, which would void anonymity (especially in New Jersey where the name of the voter is announced aloud, and challengers could easily transcribe the sequence of voters into the booths, thus providing a mapping to the printed ballots).

39. Printing out a lottery-ticket sized piece of paper with the names of the candidates that one has voted for, to be deposited in a ballot box for use in recounts, is certainly not rocket science. Over a decade ago, I had described and publicized a process by which tabulated records could be confirmed against paper ballots verified

by voters, and this has often been referred to as the "Mercuri Method." Mercuri Method - a paper ballot is prepared using an electronic voting system and displayed behind a transparent window. The voter is provided with an opportunity to verify the choices printed on the paper ballot prior to performing an action that deposits the ballot into a secured ballot box. The voter must also be provided with a way of voiding the ballot prior to casting if it is incorrect and, in such a case, must be provided with another opportunity to verify and cast a ballot.

40. These voter-verified paper ballots should be securely retained and considered to be the legal representation of votes cast. In the case where subsequent electronic tallies differ from the paper ones, the paper should prevail. The paper ballots can be printed in such fashion that allows tabulation by humans or by other computer devices (that may be supplied by independent vendors, or may be products that are openly available). As well, the paper should contain security features (such as are used with lottery tickets) to prevent fradulation or substitution.

41. It is my understanding that a voter-verified paper

ballot system such as described above, manufactured by Avante, was certified and has been available for purchase in the State of New Jersey for at least a year.

42. The country of Venezuela purchased and deployed computer systems that produced printed ballots for the voters to examine and deposit into a ballot box, in a recent election. The Carter Center concluded with confidence that the 19,000 votes they reviewed, of the over 10 million cast, were appropriately recorded and tabulated. There were no adverse experiences with paper jams (as had been rumored). Clearly, Venezuela has recognized the need for independently auditable election systems, and it is remiss that the US has not been a leader in this regard.

43. Similarly, the Sequoia Voting Systems' voter-verified paper ballot system (in which the ballots are printed on a roll) was successfully used in Nevada for a recent election, with no major problems reported. These systems will be used in many counties in Nevada for the November 2004 election.

Vendor Misrepresentation.

44. In addition to the misuse of the term "audit

trail" in order to mean something quite different from any audit that is performed in accounting or other disciplines that require independent checks, and the inappropriate claim that only "data" is on the voting machine cartridges, voting system vendors have made other false statements about their products in meetings and at demonstrations.

45. In the summer of 2004, I attended a meeting of the Mercer County Board of Chosen Freeholders where Sequoia Voting Systems' Vice President Howard Cramer claimed that

a) their voting machines were secure because no Microsoft products were used in it;

b) that the voter-verified paper trail product that they failed to supply for this November's election (which they planned to supply later) maintained anonymity of the votes; and

c) that the systems had not failed in actual use. As noted (in 38 above), the anonymity claim (b) was incorrect, and the other two statements were also false or misleading (as explained below).

46. Upon my inquiry during the Q&A session that followed the Vice President's presentation, he admitted that Microsoft products were indeed used for the ballot

cartridge programming as well as for the auditing software. This means that exploits common to those Microsoft products could be inadvertently or deliberately applied to corrupt the ballot configurations or the vote totals.

47. The claim about equipment failures was also untrue, as problems have been noted in NJ and elsewhere with their products. A recent failure occurred in a demonstration in CA, where the Spanish language ballots failed to be recorded in the vote totals. There, Sequoia Voting Systems representative Alfie Charles stated that was due to the rushed preparation for the demonstration. See Kim Zetter, Wrong Time for an E-vote Glitch, Wired News, August 12, 2004.[3] But the demonstration actually proved that it was possible to set up the machines such that certain population groups would be disenfranchised. Without a voter-verified audit trail, those missing votes would have been undetected.

48. Sequoia Voting Systems had also claimed that the machines purchased by Mercer County would be disabled accessible. Mercer County paid an additional $2,000 for each of the 300 so-called accessible machines. To date,

[3]Available At http://www.wired.com/news/evote/0,2645,64569,00.html

only a few of those machines operated properly for the disabled feature in the two elections in which they were used, so poll workers were instructed not to allow voters to use it. It is unclear that this accessibility feature will work properly in November 2004, or even by 2006 when compliance is required.

49. Although the vendors have claimed that DRE voting systems can be used by the disabled such that they can vote privately, in practice, this is actually untrue. Blind voters using Sequoia machines in California were given such instructions as "press the yellow button" by the computer voice, so that it was not possible for them to perform the operations successfully. Manhattan Borough President C. Virginia Fields, in conjunction with The Center for the Disabled in New York, released a study on the experiences of disabled voters that indicated numerous problems observed by all of the DRE types by the physically disabled. Voting Technology for People with Disabilities: A Report On Disabled Voters Experiences, (March 2003).

[**put this as a separate item under the voter-verified section above (and renumber...) -->]The U.S. Department of

Justice has deemed that voter-verified paper ballot systems will not violate rights of the disabled for equal access. Sheldon Bradshaw, Whether Certain Direct Recording Electronic Voting Systems Comply with the Held America Vote Act and the Americans with Disabilities Act: Memorandum Opinion for the Principal Deputy Assistant Attorney General Civil Rights Division (October 10, 2003). Furthermore, there are tactile ballots (used in Rhode Island and approved by the United Nations) that allow visually impaired and illiterate citizens to vote privately without computers.

50. This is but a short list of misrepresentations that have occurred with vendors for election products, there are many others on record.

Summary of Testimony.

a) Based on my expertise in the fields of computer security and real-time interactive computer systems and the research I have conducted on electronic voting systems over the past 15 years, I can attest to the fact that it is currently not possible to confirm that electronic voting systems are performing properly during elections.

b) Electronic voting systems are not fail-safe and are capable of malfunctioning in such ways that could alter or destroy ballot images, corrupt vote totals, or make the voting stations unavailable during the election period. Instances of such occurrences in actual elections have been confirmed.

c) It is not possible to determine if an electronic voting system has been internally corrupted because DRE source code is protected from scrutiny by manufacturers' claims of trade secrecy and the inadequacy of functional tests. Functional testing processes performed prior to an election do not reveal many hardware or software problems that could cause systems to function inappropriately during an election.

d) Analyses of the set-up procedures and components of DRE voting systems have revealed that these systems are physically vulnerable, creating insecurities that can be exploited to allow the manipulation of election results. These flaws have been brought to the attention of manufacturers who have misrepresented the seriousness of these weaknesses and have not taken action to improve the integrity of these systems.

e) Studies have shown that fully-electronic voting systems can have higher residual (missing or unrecorded) vote rates than optically scanned paper balloting systems, and the reasons for this are currently unknown. Without any way to independently verify the correctness of the vote tallies, it may be the case that a percentage of votes cast (large enough to affect the outcome of a race) may not be reported.

f) In order to assure that DRE voting systems are secure from tampering and function properly it is critical to perform comprehensive white and black box testing of voting systems, as well as functional testing, for all equipment deployed for use.

g) Since the DRE voting systems provide no independent way to verify correctness, the only currently available solution for auditing involves the addition of voter-verified paper ballots. As well, the optically scanned paper ballots must be audited because the systems used to collect their vote totals are equally vulnerable to many of the issues that have been discussed herein.

_____

Rebecca Mercuri, Ph.D.

Dated: Lawrenceville Township, New Jersey
October 16, 2004

Exhibit B- Glossary of Terms

Components of Electronic Voting Systems.

Regardless of their brand, electronic voting systems share many similar components. The voting process on electronic voting machines, and key software is defined below to facilitate the Court's understanding of DRE voting systems.

- The voting terminal (also known as a Direct Record Entry device, or DRE) is the device in a voting system that runs the system's vote collection software. It includes a variety of components such as: the data entry device (a touchscreen or button panel), ballot recording mechanisms (write-once memory chips or disks), the object code that runs the device, a printer to display election totals, and vote counter.
- Microprocessor (processor or Central Processing Unit, CPU) -- this is the "brain" of the voting system. It accepts instructions that were previously encoded into a numeric format, and executes them in conjunction with data (also encoded numerically).
- Source code is the untranslated set of instructions that will be converted into the object code that makes the voting

system operational. Computer professionals create the source code using languages that are human readable. Source code also usually includes comments to enhance human understanding of the software, but these are not reflected in the object code. Changes in source code may result in changes in object code that can affect the behaviour of a voting machine.

- Object code is the translated version of the source code instructions that are used by the voting terminal to perform its functions. Object code is generally not human readable and is also not a one-to-one correspondence with source code, but rather a numeric tranformation specific to the microprocessor being used. Many of the details of the source code are lost when the translation is performed, and there is typically a large percentage of source code that may look different but will translate to the same object code. Although source code is generally thought of when people refer to "software" they actually mean the object code, because microprocessors cannot directly execute source code.
- A compiler is a computer program used in the development of a voting system that provides the translation of source code into object code. A compiler typically also performs optimization in order to make the code execute more

efficiently, so that it is generally not possible to retranslate the object code back into the source code.

- The data storage area is located inside the voting system. It may consist of a removable medium (such as a magnetic disk, CD, or memory card or cartridge. The data is stored in an encoded numeric format and may include object code instructions, configuration information, tables, back-up copies of ballot images and vote totals, and voting audit logs.
- Audit logs are created inside of the voting system when certain (but not all) functions are performed. These may include start-up and closing times of the voting system, and ballot images (encoded records of the selections made by individual voters). Critical items that are often not included in voting system audit logs may include indications that the system has been modified (because generally the computer is not powered on when this is performed), the names of persons who have had access to the internals of the system, and the sequential record of all of the actions made by the voters (because this would void the anonymity of their ballots).
- Removable flash memory devices/or cartridges are memory

storage devices similar to computer disks. They are inserted into a portal inside some voting terminals to store voting records (votes cast at the terminal) and voting audit logs. These devices are detachable and can be transported to other locations where systems can read their contents in order to prepare the election totals. Some flash memory devices are of sufficient capacity that they may also contain object code instructions along with ballot data. There may not be any protection mechanism in the device that prohibits its contents from being altered.

- Encryption is a process of encoding data to limit access to it. Encryption, when done properly, ensures that only authorized individuals are able to access system components and data. In actual practice, encryption methods often become obsolete over time because of techniques developed to circumvent it, so the encrypted information can be revealed by unauthorized persons. There are voting systems currently in use that contain such obsolete encryption methods. Typically a password or set of passwords is used with encrypted information, and the misuse of these passwords can also provide voting system vulnerabilities.

Prior to an election, voting terminals must be configured and installed at polling locations. Configuration may include attaching each voting terminal to a central computer, and/or it may involve the transfer of data and object code instructions via memory devices (such as cards or cartridges). Part of the installation of a voting terminal is the loading of the ballot definition file to be used during the election.

- Ballot definition files are computer files that contain the offices and issues to be voted upon during the election, as well as the names of the candidates and their parties. These definitions may be in an encoded format that also includes instructions pertaining to how the candidates will be displayed on the voting device. Ballot definitions may be installed into the voting terminal by inserting a memory device or by direct or networked connection to a central computer.
- A ballot image is the numeric encoding of a particular set of candidate (and referendum question) selections made by a voter. The ballot image may not show the actual candidate names, rather a mapping may be used.

Voting systems may use dedicated networks (known as Local Area

Nets or Wide Area Nets) to transfer information such as the ballot definition files and the vote audit data. These networks may vulnerable to monitoring or spoofing (a bogus network pretending to be the real one) and may also be attachable to the Internet where uncontrolled actions may occur.

In order for voters to cast votes they must check in at the polling place. Some DRE voting systems require that voters access the machine by using a voter Smartcard.

- A voter card/"Smartcard", is a credit card sized plastic unit with a magnetic strip and computer chip that can store data.

If Smartcards are used, once inside the voting booth, the voter must insert the Smartcard into a Smartcard reader that is housed with the voting device. Special smartcards may also be issued to election administrators so that they can access the machines to perform administrative functions.

- Smartcard Readers communicate voter authentication information to the terminal, and activate terminals. The information read from the smartcard may also instruct the terminal to display the proper ballot.

In the case of a touchscreen machine, if the system is presented with a valid voter card it will display the ballot and allow the voter to vote. In the case of a full-face ballot display, the voter registers their selections by pressing buttons that are concealed behind a large piece of paper that maps the buttons to candidate's names. It is possible that the mapping on the paper may be incorrectly correlated with the internal mapping of the buttons to particular candidates.

- File Servers are the central computers maintained by the county (and in some cases the vendor of the voting system). These servers may be used for various functions (such as the repository for ballot definition files) and may also send and receive data (that can include object code, ballot images, and vote totals) to/from the voting terminals. A tabulating procedure may be used by the central computer to determine a final summary election results from the individual voting records collected from each of the voting terminals. Nothing prohibits file servers from being connected to other systems (providing high vulnerability), and some may be used to provide direct feeds to press agencies or to generate Internet postings at the end of the election.