Mr. Howard T. Van Pelt, CEO
Advanced Voting Solutions, Inc.

Mr. Kevin Chung, President and CEO
Avante International Technology, Inc.

Ms. Conny McCormack, Registrar of Voters
County of Los Angeles

Mr. Bruce Krochman
DFM Associates

Mr. Walden W. O'Dell, Chairman, President and CEO
Diebold Election Systems, Inc.

Mr. Randall Rattray
Election Data Direct

Mr. Aldo Tesi, President and CEO
ES&S

Mr. David E. Hart, Chairman
Hart InterCivic

Scott Martin, President
Martin & Chapman

Tracey Graham, President
Sequoia Voting Systems

Mr. Jack Gerbel, President
Unilect

Dear Ladies and Gentlemen:

As you are aware, earlier this year I formed the Secretary of State's Ad Hoc Touch Screen Task Force in response to concerns over the security of Direct Recording Electronic (DRE) voting machines and the issue of whether to require each machine to include a voter verified paper trail. Enclosed is my position paper outlining how I intend to proceed on this issue.

In brief, I am requiring that as of July 1, 2005, all local jurisdictions purchasing new DRE voting systems may only purchase certified DRE voting systems that contain a VVPAT feature which is fully accessible and allows every voter—including disabled voters and those speaking English as a second language—to vote privately and independently. Accessible means that the information provided on the paper printout from the VVPAT mechanism is provided or conveyed to voters via a non-visual method, such as through an audio component.

As of July 1, 2006, DRE systems already in use on that date will have to be replaced or modified to incorporate an accessible VVPAT feature, if they do not already contain one. I am directing the Voting Systems and Procedures Panel to develop standards for the printed ballot copy – which will be the

In addition, all new DREs purchased after July 1, 2005 must also include electronic verification as the means to assure that the information provided for verification to disabled voters accurately reflects what is recorded by the machine and what is printed on the VVPAT paper record. Any

electronic verification method must have open source code in order to be certified for use in a voting system in California. The Voting Systems and Procedures Panel will work with a soon-to-be named Technical Oversight Committee to establish standards for electronic verification.

While I am convinced that the voting systems certified for use in California are secure, I recognize that security can and must always be strengthened. Therefore, in order to augment current security procedures, I will be adopting stricter standards at the state level, imposing additional security requirements on voting system manufacturers and urging the federal government to improve their testing standards and procedures.

I must also ask for the cooperation of you and the other voting system manufacturers to augment security protocols and procedures in the development, manufacturing, distribution, and implementation of voting systems. The following are the key recommendations that I will implement that have the most direct effect on voting machine manufacturers:

1. **Only Certified Software** - Local jurisdictions may not utilize systems with equipment or software that have not been fully certified. This means no one may alter software that has not been certified for use by the State, and the distribution of qualified voting system software must be tightly controlled. Therefore, the State, and not vendors, will control the distribution of object code to every local jurisdiction. My office will soon provide procedures to clarify how this will occur.

2. **Logic & Accuracy Testing** - The Logic and Accuracy process conducted at the local level must be as reliable as the Federal and State tests. As such, the system vendor may not conduct these public tests, but rather, they must be conducted by county elections personnel.

3. **Review Screen** - In order to minimize unintentional "undervotes," voters must be provided with a review screen on all DRE systems that provide them a reminder that they have not voted in or have skipped a particular race. This must also occur on any accessory providing access to the disabled such as a voice-guided audio ballot system using headphones and a keypad.

4. **Background Checks** - In order to assure that vendors are using programmers and designers of software that have only a commitment to creating the best product, and to prevent easily foreseeable problems for individuals with a clear history of criminal activity and/or mental instability, manufacturers who seek certification of a system in California will be required to conduct background checks of programmers and developers before they are hired to work on election system software. My office will establish standards for these background checks, and will require that results of the checks be made available to the State upon request.

5. **Internal Security** – My office will establish protocols and procedures for manufacturers to comply with, in order to guarantee that strict internal security procedures are used

during their software development process. Manufacturers shall be required to submit employee and other internal security procedures with their certification materials.

6. **Chain of Custody** – I am requiring that manufacturers document a clear chain of custody for the handling of software to assure that all software and storage units containing software are handled, tested and transported in an appropriate manner. In addition, transfers of software over the Internet will be prohibited. My staff will provide guidance to all manufacturers on these issues.

7. **Civil Liability** – I will seek legislation to impose civil liability and stiff criminal penalties if any malicious code is found in a voting system before, during, or after certification, whether such malicious code interferes with an election or simply was intended to interfere.   This effort is based on the concerns of many people that employees of manufacturers are a threat to the security of voting systems. I would urge your company to support this effort to assure greater confidence in our voting systems.

My office will provide more detail on each of these items to you by December 31, 2003, in an effort to increase security of voting systems in California and across the nation. I urge your company as well as your competitors to join me in the effort to increase confidence in our voting systems and work with me to implement these new procedures and requirements.

Please feel free to contact me in the future with any other concerns you may have.

Sincerely,

KEVIN SHELLEY
Secretary of State