HART
intercivic™

July 17, 2005

Ann McGeehan
Director of Elections
Secretary of State
1019 Brazos Street
Austin, TX 78701

Dear Ms. McGeehan,

Your letter dated July 14, 2005 contained two questions from the voting system examiners concerning the use of a software utility and the function of the security key. I have provided responses to those questions below.

1. The utility in question is a development tool used by Hart InterCivic to reset our hardware components during our internal development and test efforts. The utility should not have been present or used during certification and the concerns expressed by the examiners are justified. The function performed by this utility is provided to our customers by SERVO, a submitted and certified product that supports the reset capability. SERVO embodies Hart InterCivic's security policies requiring user name and password along with the electronic key as demonstrated during the examination for the other PC-based applications and described below.

2. The USB key is used to digitally sign data whenever the data is moved from one system component to another. This is done to ensure that when the data is outside the authenticated environment of the system components, it cannot be changed or modified without detection. When the data is within a system component, it is secured by the system authentication requirements, the Principle of Least Privilege, Segregation of Duties, and Role-Based Privileges. The USB key is not required to be in place at all times, for example when an operator is entering and editing the ballot definition in BOSS there is no need for the application to access to the USB key. The USB key is required when the ballot definition is complete and the ballot is generated to create the ballot data for the MBB. When the ballot data file is created for the MBB, the USB key provides the two-factor security. The USB key, which is under physical control by the election administrator, is used to digitally sign the election data that is written to the MBB and used by all subsequent system components. When the other system components read the MBB data, they use the key to authenticate the data on the MBB. In a similar fashion, when other system components such as Ballot Now, eScan, or the JBC add Cast Vote Records to the MBB, the Cast Vote Records are digitally signed so that the data cannot be altered or modified without detection. When the MBBs are read into the authenticated environment

of the Tally system component, Tally authenticates the data on the MBB using the USB key. Please refer to the Symantec white paper "Securing the eSlate Electronic Voting System Application Security Implementation" (attached) for further details of the comprehensive security surrounding the Hart Voting System.

Please let me know if these responses satisfy the examiner's questions or if additional follow up is required.

Sincerely,

Neil McClure
Vice President
Hart InterCivic, Inc.