M E M O R A N D U M

TO: Supervisors of Elections

FROM : Dawn K. Roberts, Director

DATE: March 3, 2006

SUBJECT: Technical Advisory

Purpose:
This advisory concerns enhancements to voting system security procedures that each supervisor of elections must address immediately. Provided within this technical advisory are guidelines that clarify the requirements for meeting the minimum security standards of 1S-2.015 (5)(g), (k) and (n).

Background and Scope:
Florida's voting systems standards and certification program are recognized as the most stringent in the nation. Supplementing this rigorous certification process are the detailed security procedures that each county supervisor of elections must establish and follow. Indeed, the success of a certified voting system is largely dependant upon the security employed.

As a matter of practice, Florida's voting systems standards and certification program are reviewed by the Division's Bureau of Voting Systems Certification on a continuous basis. The Bureau recognizes that as technology evolves so must our security procedures surrounding the operations of our voting systems. As we identify new procedures and guidelines that are necessary, it is paramount that county Supervisors amend their security procedures.

In addition to the Division's ongoing internal examination of security procedures, we have recently reviewed the State of California's Voting Systems Technology Assessment Advisory Board's (VSTAAB) Security Analysis of the Diebold AccuBasic Interpreter and Ciber Laboratory's Source Code Review and Functional Testing reports. The Florida Division of Elections believes that potential system vulnerabilities identified in these reports can be addressed through enhanced security safeguards. In general, these recommendations are applicable to all types of election media including compact flashes, PCMCIA cards, memory packs, PEBs, and paper ballots. **This technical advisory therefore applies to all voting systems deployed in Florida.**

Note that the use of the word "procedure" within the context of this technical advisory means a macroscopic description of a process that defines the duties, responsibilities, and activities of an individual or a group of individuals. While explicit step-by-step task specific work instructions necessary for implementation are not required to be included in

your revised security procedures when submitted to the Division of Elections for approval, such instructions must be incorporated into your county's overall security plan to ensure the highest level of system protection.

Recommendations and Guidelines

Pre-election Steps for Voting Systems:

Threat model and mitigating strategy:

When developing a security procedure, one should determine the key elements within a system and develop threat models against those elements. For example, consider a threat model that consists of a "knowledge based" attack focused on a scanner memory card or any other type of election media. This "knowledge based" attack assumes that the security perimeter surrounding this media can be breached to allow unfettered access or that an internal party utilizes their position of responsibility to gain such access to the media. The mitigating strategy to defend against such an intrusion includes one or more security layers focused on election media accountability and chain of custody. Therefore, the following guidelines serve as the minimum criteria for evaluating compliance to this security procedure element as it relates to electronic media.

1) Regardless of electronic media type (memory packs, compact flash cards, PC Cards [aka PCMCIA cards], PEBs, voter card encoders, supervisor cards, and key cards), all such media shall be permanently identified with a unique identification (e.g., serial number).
    a. The supervisor of elections shall create and maintain an inventory of all electronic media.
    b. The supervisor of elections shall create a process and maintain a procedure for tracking the custody of electronic media from their storage location, through election coding, through the election process, to their final post-election disposition and return to storage. This electronic media must be given the same level of attention that one would give to official ballots.
    c. The chain of custody must utilize two or more individuals to perform a check and verification check whenever a transfer of custody takes place.
2) The supervisor of elections shall create and maintain a secured location for storing the electronic media when not in use, for coding an election, for creating the election media, for transferring and installing the election media into the voting device, and for storing these devices once the election parameters are loaded.
    a. No election media shall be left unattended or in an unsecured location once it has been coded for an election.
        i. Where applicable, coded election media must be immediately loaded into the relevant voting device, logged, and made secure or must be placed in a secured and controlled environment and inventoried.
    b. For each election, the supervisor of elections shall seal each election media in its relevant voting device or container utilizing one or more uniquely identified tamper-resistant or tamper-evident seals.
        i. A combined master identification of the voting device, the election media, and the seal(s) must be created and maintained.

ii. For election media that are device independent (e.g., PEBs, voter card encoders) these devices should be stored in a secured, sealed container and must also be identified on a master log.

c. The supervisor of elections shall create a process and maintain a procedure for tracking the custody of these voting devices once these devices are loaded with an election definition. These voting devices must be given the same level of attention that one would give to official ballots.

d. The chain of custody must utilize two or more individuals to perform a check and verification check whenever a transfer of custody takes place.

3) The supervisor of elections shall have in place a recovery plan that is to be followed should there be any indication of a security breach in the accountability and chain of custody procedures. Any indication of a security breach must be confirmed by more than one individual.

4) The supervisor of elections shall have a training plan for relevant election officials, staff, and temporary workers that address these security procedures and the relevant work instructions.

Transport of Ballots and/or Election Materials:

Threat model and Mitigation Strategy:

Consider a threat where a malicious entity wishes to gain access to a memory card or any type of election media. This could occur at any time prior to opening the polls and with the election media in any state (i.e., pre-election, set for election, or post-election.) The mitigating strategy to defend against such an invasion includes one or more security layers that again focus on accountability and chain of custody. Therefore, the following guidelines serve as the minimum criteria for evaluating compliance to this security procedure element.

1) The supervisor of elections shall create and maintain a secured location for storing and transporting voting devices once the election parameters are loaded. This shall include procedures that are to be used at locations outside the direct control of the supervisor of elections, such as overnight storage at a polling location.

a. For each election, the supervisor of elections shall create and maintain an inventory of these items for each storage location. These voting devices must be given the same level of attention that one would give to official ballots.

b. The chain of custody must utilize two or more individuals to perform a check and verification check whenever a transfer of custody takes place or where the voting devices have been left unattended for any length of time. Particular attention must be given to the integrity of the tamper-resistant or tamper-evident seals.

2) The supervisor of elections shall have in place a recovery plan that is to be followed should there be any indication of a security breach in the accountability and chain of custody procedures. The plan must also address inadvertent damage to any seals or accountability/chain of custody documentation errors. These plans must be developed in a manner that enhances public confidence in the security and integrity of the election. Any

indication of a security breach, documentation errors, or seal damage must be confirmed by more than one individual.

3) The supervisor of elections shall have a training plan for relevant election officials, staff, and temporary workers that address these security procedures and the relevant work instructions.

Election Access to Voting Systems:

Threat model and Mitigation Strategy:

Consider a threat model to optical scanners, DRE touchscreens, central count scanners, and the election management system; the success of which relies on a known vulnerability in an election department's security protocols. Under this condition, perimeter security may be compromised where access to the voting system relies on default passwords and encryption keys or where such items are not changed frequently. The obvious mitigating strategy to defend against such an intrusion includes immediately changing the default passwords and encryption keys and to develop a plan and process for changing the access control built on some time-based or event-based characteristic. Therefore, the following guidelines serve as the minimum criteria for evaluating compliance to this security procedure element.

1) The supervisor of elections shall have a procedure that ensures that default or vendor supplied passwords, encryption keys, etc. have been changed.
   a. The supervisor of elections must maintain these access control keys/passwords in a secured and controlled environment. Who has access to these items must be delineated in the relevant position descriptions.
   b. Changes to the encryption keys and passwords are at the discretion of the supervisor of elections, but it is advisable that this discretionary authority should not be delegated. However, the individual(s) that implement the change must have this "authorization to change" responsibility delineated within their position description(s). *(Note the distinction relative to describing who can authorize a change, who implements a change, and who has access but cannot change the passwords and encryption keys.)*
   c. Where appropriate, the degree of access should be defined within each relevant position description and maintained at that level within the election management system and/or equipment. This applies where a voting system can limit an individual's access to certain menus, software modules, etc.
2) Access to any device, election media, or election management system that requires the use of an encryption key must be witnessed by one or more individuals authorized to use such information.
   a. An access log should be developed and utilized.
3) The supervisor of elections shall have a training plan for relevant election officials, staff, and temporary workers that address these security procedures and the relevant work instructions.

Specific Authority: 101.015 F.S.
Rule: 1S-2.015 (5)(g), 1S-2.015 (5)(k), and 1S-2.015 (5)(n)