System Security

Election Management Guidelines

A presentation to the
EAC Commissioners

April 18, 2007
Brit Williams

Thank you for the opportunity to participate in the Election Management Guidelines project. I have been involved with elections since 1986. During that time I have participated in the development of all of the various voting system standards and served on the NASED Voting Systems Board; however, the Election Management Guidelines project is, by far, the most exciting and far-reaching project with which I have been involved. For the first time, we are developing a comprehensive assistance tool for the grass-roots election official. To date, we have developed the first three chapters of these Guidelines. I am going to give a brief overview of Chapter 2, System Security.

Overall security of a computer-based voting system is enhanced by a combination of four factors working in concert with each other:

1. *Use of software that limits its application to the very basic functions required to perform the voting system's processes.* Additionally, the software should provide audit scripting that is sufficient to track the sequence of events that occur on the system and, to the extent possible, identify the person(s) that initiated the events. The software should also employ a sufficient level of encryption or validation protocol to limit the ability of the software to accept changes without proper authorization and still function correctly;

2. *Use of well defined and strictly enforced policies and procedures controlling access to the voting system, the circumstances under which users can access the system, and the functions they are allowed to perform on the system.* Strong custody control of all equipment, software and key or control materials must be maintained at all times;

3. *Use of physical security and access logs.* Physical security includes fences, walls, doors, locks, seals, etc., that control and limit access to the system;

4. *Use of two person accountability and control*. Access, control and custody should always involve two or more personnel. This is to independently verify the honesty and integrity of the election procedures under any scrutiny.

For each of theses factors there is no "one size fits all". What might be appropriate policies and procedures for a large election office with over a dozen staff members may be overly burdensome for a small, two-person election office. The *Election Management Guidelines* provide guidelines for implementing these four factors within the election environment.

Chapter 2, System Security, contains recommendations for Software Security, Policies and Procedures, and Password Maintenance.

The first step in voting system security is to be sure that you install the correct version of the software (i.e. the version certified by the EAC). Thereafter, the software must be constantly monitored for evidence of fraudulent or accidental modification. In the Software Security section there are guidelines for installing a voting system in a manner that will insure that the installed system is identical to the EAC certified version of the system and for using the NIST National Secure Reference Library to periodically and randomly verify that the system has not been altered. This section also provides guidelines for the transmission of unofficial results over telephone circuits and the use of the voting system's audit data.

Over time, especially during the preparation and execution of an election, there are many people that have access to various parts of the voting system. These include election office staff, vendor personnel, and voters. The Policies and Procedures section stresses the importance of having well-defined and strictly enforced policies and procedures for every person that has access to the voting system.

Effective use of passwords is essential to the overall security of a voting system. Passwords are the primary tool used to restrict a person's access to the voting system to only those portions of the system necessary for their job responsibility. Passwords are also used to restrict unauthorized access to the voting system. The Password Maintenance section recommends that either the Chief Election Officer or a senior member of the staff be designated as the Password Administrator. The duties and responsibility of the Password Administrator are defined. Guidelines are presented for issuing passwords, maintaining a master list of passwords, re-issuing passwords on a periodic basis, and monitoring password usage.