CHAPTER 2

SYSTEM SECURITY

Introduction

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

- ★ *Use of software should be limited to the very basic functions required to perform in the voting system's processes.* In addition, the software should provide audit scripting to track sequence of events that occur on the system and, to the extent possible, identify person(s) that initiated the events. The software should also employ a sufficient level of encryption or validation protocol to limit changes made without proper authorization.
- ★ *Use well-defined, strictly enforced policies and procedures to control access to the voting system, the circumstances under which users can access the system, and functions users are allowed to perform on the system.* Maintain strong custody control of all equipment, software, and key or control materials at all times.
- ★ *Use physical security and access logs.* Physical security, including fences, walls, doors, locks, seals, and so forth, control and limit access to the system.
- ★ *Use a two-person accountability and control system.* Access, control, and custody should always involve two or more personnel. This accountability independently verifies the honesty and integrity of the election procedures under any scrutiny.

There is no "one size fits all" for each of these factors. 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 following sections provide guidelines for implementing these four factors within the election environment. Factors that are considered important will be clearly indicated. A range of acceptable factors are presented where possible.

Software Security

Initial Installation. The first step in securing voting system software is ensuring that the software installed on the system is the exact software version that has been certified by your State or the Federal certification program. The most straightforward way to accomplish this task is to obtain the software directly from your State elections office or the Voting System Test Laboratory (VSTL) that performed the tests for EAC certification.

It is not uncommon to find an election office in which the voting system has been installed for a considerable length of time, during which the vendor has had access the system unsupervised by an election official. In circumstances such as this, strongly consider the following recommendation:

- ★ If you suspect that the voting system software has been compromised, reinstall the voting system software with a copy of the software obtained directly from your State elections office or the VSTL that performed the tests for EAC certification.

As the last act, a VSTL produces a "final build" or "trusted build" of the system. The output of this final build is a CD that contains the system source code, the object code, and various documents. In addition, they also produce a self-loading disk that can install the system on your computer.

- ★ A copy of the self-loading disk is required to reinstall the system. If the State election office does not have the disk, it can obtain the disk by requesting that your vendor authorize the Independent Testing Authority (ITA) that performed the certification tests on the system to send the

disk to the State office or directly to you. If you are unsure about how to install the disk, contact your State election office for instructions and help.

★ The self-loading CD installs the election management system on the central election computer. If the firmware in the voting stations or ballot scanners needs to be reinstalled, ask your vendor what you need from your State election office or the ITA. The device will probably be a PCMCIA (Personal Computer Memory Card International Association) card or a similar device.

Although it is important for the voting software to be complete and correct, it is equally important that the voting system software is the *only* software on the vote-tabulating computer.

★ Do not allow any software on the vote-tabulating computer except for the voting system software itself. Specifically, do not allow office automation software such as Microsoft Word, PowerPoint, Excel, and so forth, or networking software such as e-mail, network browsers, and so forth.

Periodic Monitoring. After the voting system is correctly installed, processes and procedures need to be implemented to keep the software secure.

The National Institute of Standards and Technology (NIST) offers a secure software repository, the National Secure Reference Library (NSRL). This service enables election personnel to check periodically that the installed software has not been altered.

NIST obtains a copy of each voting system from the EAC VSTL and computes a digital signature of the system. NSRL can create the same digital signature for your system and compare it to the signature in the NIST library. This comparison will reveal any alteration to the system.

★ The Web site for this service is **www.nsrl.nist.gov/votedata.html**. On this Web site is a list of voting systems that have been submitted to NIST for inclusion in the NSRL. If the version of the voting system you are running is not on this list, request that your vendor submit the system or system version to NSRL.

★ Even if your voting system is on this list, it is unlikely that you will be able to complete the comparison without help. The EAC office can provide you with a contact at NIST that can assist you.

Founded in 1901, NIST is a nonregulatory Federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. For more information about NIST, visit their Web site at **www.nist.gov** or call them at 301.975.NIST (6478).

Networking. The possibility of fraudulently altering voting system software is based on the assumption that hackers have access to the system. This type of voting system attack can be avoided by never connecting the voting system to any network not under your complete control. This includes the Internet and any local network unless the network is wholly contained within your facility and is controlled by a trusted organization.

★ Never connect a voting system component to any network not under your direct control. All unused connections on the permanent systems should be sealed, precluding unapproved network, modem, USB, parallel, or other port connectivity.

Modem Transmission of Unofficial Results. The caution about not permitting network access does not apply to the use of modems on election night to transmit *unofficial* polling place results to the central office. The technical expertise required to intercept and alter a telephone communication without detection is extremely complex. Therefore, it is unlikely that anyone will be able to intercept and alter these results without detection. Even if the unofficial results are intercepted, it would make no difference in the final, official results since these should never be sent via modem. The official results should always be computed from the media that is physically transported from the polling place to the central office.

★ If modems are used to transmit polling place results to the central office, consider these results to be unofficial, and always verify them against the results on the media that is physically transported to the central office.

Audit Data. A voting system has several different audit logs. These logs contain a record of each event that occurs on the system from the time used to initially begin an election until the final

vote tally is completed. Audit logs on precinct-based voting equipment begin at the time the election media is inserted into the device until the election is closed.

- ★ Review the audit log documentation or obtain from your vendor a complete description of the audit logs that are available on the voting system. Familiarize yourself with the content of these logs and learn to print them out.
- ★ As part of pre- and post-election activities routine, print and examine these audit logs.

Policies and Procedures

A well-defined procedure for monitoring each person with access to the voting system should exist.

Examples of criteria to apply to voters who have access to the voting system are as follows:

- ★ A clear definition exists of who exactly qualifies as a voter.
- ★ A system exists for maintaining a record of each voter (i.e., the registration system).
- ★ A record is maintained of each time the voter uses the voting system.
- ★ The voter can use the voting system only at a specified, well-defined time (i.e., in-person absentee voting, in-precinct voting, early voting, etc.).
- ★ The voter must follow a well-defined and rigorously enforced procedure before he or she can use the voting system.
- ★ The voter's use of the voting system is restricted to only one function on the voting system: casting a ballot.

Equally specific procedures should be developed for each person that has access to the voting system. This includes elections office staff, vendor personnel, and visitors.

- ★ Require positive identification of each person that requests access to the voting system.
- ★ Keep a log of everyone that accesses the voting system. This should include the person's name, the date and time the access begins, the purpose of the access, and the time the access ends.
- ★ Access log entries should be written by someone other than the person accessing the system. The entries in this log must be complete and detailed. For example, "System Maintenance" is not an acceptable entry. The entry should state the exact maintenance performed and the reasons why it was performed.

Elections Office Staff. Elections office staff should only be allowed the level of access to the voting system that is necessary for them to perform specific tasks related to their job description. Do not issue a staff member a password that will allow him or her to perform functions on the voting system that he or she is not authorized to perform. It is highly recommended that whenever possible, elections staff work in pairs. This procedure will greatly reduce the potential for accidental errors and virtually eliminate any opportunity for deliberate mischief or fraud.

Vendor Personnel. There is no such thing as "routine system maintenance." The vendor can void the voting system's Certification by making a change to the system that has not been approved by the State or the EAC.

- ★ Never allow vendor personnel access to your system until you are absolutely certain that any change, upgrade, or maintenance they intend to perform has been approved by the State or the EAC. All approved modifications or upgrades to an EAC certified voting system are documented with a certificate. If the vendor cannot produce a copy of this certificate do not allow him or her to access the voting system. When in doubt, call the EAC for clarification.
- ★ Never allow vendor personnel to access the voting system unless a member of the election staff is present. Although it is recommended that election office staff work in pairs, it is essential that the vendor never be allowed access to the voting system without a member of the election office staff present. Emphasize to the vendor that this requirement is as much for their protection as it is for yours.

Everyone else. There is absolutely no reason—*Never, Under Any Circumstances*—to ever allow anyone other than election office staff or vendor personnel access to the voting system. A consultant working under contract to the election office is considered election office staff; however, consultants should be monitored as closely as vendor personnel.

Password Maintenance

Effective use of passwords is essential to the overall security of a voting system. The first step in managing passwords is to know exactly what password capability is available on the voting system. The EAC Voluntary Voting System Guidelines Section 7.2.1 General Access Control Policies states, *"…the vendor shall provide a description of recommended policies for effective password management."* Obtain this description from the vendor and provide a copy to every employee authorized to access the voting system.

The following sections provide guidelines for effective password management.

Password Administrator. Designate someone in the election office as the password administrator, either the Chief Election Officer or a senior member of the staff. The password administrator's duties are as follows:

- ★ Issue passwords.
- ★ Maintain a master list of all passwords issued.
- ★ Reissue all passwords periodically.
- ★ Monitor password usage.

Issuing Passwords. Passwords issued to employees should only allow them access to the portion of the system required to do their job. The password administrator or the individual employee can make up these passwords. Passwords should have the following characteristics:

- ★ Passwords should be at least six characters long, preferably eight.
- ★ At least one character should be an uppercase letter.
- ★ At least one character should be a lower case letter.
- ★ At least one character should be numeral.
- ★ At least one character should be a special symbol.

Remember that passwords are case sensitive. For example, ABC*123# and Abc*123# are different passwords.

Passwords should be easily remembered (so there will be no need to write them down) yet sufficiently vague that they cannot be easily guessed. It is best to avoid the use of personal information (name, date of birth, anniversaries, pet's names, etc.) and the use of real words (certain technology enables individuals trying to predict passwords the capability of trying every word in the dictionary). It is best to use a mix of different character types (uppercase, lower case, numbers, and symbols).

Never issue a system password to anyone other than an election office employee, not even vendor representatives. If someone other than an election official needs to access the system, either have an election official log in for him or her or create a dummy password and then delete it as soon as the session is over. (Remember, someone from the elections office staff should monitor all vendor and consultant access to the system and log this activity, including date, time, names, and reason for access.)

Maintaining a Master List of Passwords Issued. It is OK to allow individual employees to make up their own passwords; however, they must submit their passwords to the password administrator for inclusion in the master list. The password administrator should verify that the passwords comply with the requirements above. The password administrator should compose a master list of all passwords issued. A printed copy of this list must be kept in a safe and secure place and should only be used in the event of an office emergency. Even in the event of an emergency, use of the list should be restricted to the Chief Election Official and the password administrator.

"Safe" and "secure" do not mean the same thing. A fireproof filing cabinet may be safe, but it is not secure unless it is locked and access to the key is restricted to the Chief Election Official and the password administrator. Similarly, an encrypted file as a backup on a disk drive may be secure, but it is not safe. Disk drives can fail.

Reissuing Passwords on a Periodic Basis. Password protection is good but not infallible. All passwords should be changed on a periodic basis. A recommended period is one election cycle or at least once a year.

Monitoring Password Usage. Election employees' password usage should be monitored. Devise monitoring activities that are appropriate for your office, but consider things such as the following:

- ★ Watch for passwords on post-it notes posted on the side of monitors or in desk drawers. To avoid this, choose passwords that are easy to remember. Remind staff that if they do forget their password they can get it from the password administrator.
- ★ Review audit logs to verify that employees are working only within their assigned responsibilities.

Most systems allow employees to change their password at any time. Require that employees obtain prior permission from the password administrator before changing their password. Perform random checks to verify that passwords are changed with the password administrator's approval. One verification option is for the password administrator to attempt to log in with each employee's password in the master list. If the password has been changed, the password in the master list will be invalid.

Page is intentionally left blank