U.S. Election Assistance Commission

Election Management Guidelines

www.eac.gov

U.S. Election Assistance Commission

Election Management Guidelines

Acknowledgments

The U.S. Election Assistance Commission thanks the election officials in the following jurisdictions for their time, energy, and experience in making this document both meaningful and usable by the election community in the United States.

Local Election Jurisdictions

Arlington County, VA
Augusta County, VA
Cerro Gordo County, IA
Chelan County, WA
Chesterfield County, VA
Citrus County, FL
City of Charlottesville, VA
City of Danville, VA
City of Richmond, VA
Clark County, NV
County of Henrico, VA
Dallas County, TX
Denver County, CO
District of Columbia
Fairfax County, VA
Forsyth County, GA
Franklin County, OH
Guilford County, NC
Halifax, VA
Harris County, TX
Hinds County, MS
Lane County, OR
Larimer County, CO
Linn County, IA
Marion County, OH
Mecklenberg County, NC
Miami-Dade County, FL
Montgomery County, MD
New Castle County, DE
New York City, NY
Orange County, NC
Richmond County, GA
Sacramento County, CA
Santa Ana, CA
Santa Fe, NM

State Election Offices

State of Arizona
State of Florida
State of Iowa
State of Kansas
State of Louisiana
State of Maryland
State of Michigan
State of Missouri
State of North Dakota
State of South Carolina
State of Wisconsin

Organizations of Election Officials

EAC Advisory Board
EAC Standards Board
The Election Center
The International Association of Clerks, Recorders, Election Officials, and Treasurers
The National Association of Secretaries of States
The National Association of State Election Directors

Contents

Introduction

"The conduct of elections, for many citizens, constitutes their only participation in government, and it is fundamental that elections be properly conducted." ~ Joseph P. Harris, "Election Administration in the United States," 1934

Background

The Help America Vote Act of 2002 (HAVA) established the U.S. Election Assistance Commission (EAC) to "assist in the administration of Federal elections and to otherwise provide assistance with the administration of certain Federal election laws and programs, to establish minimum election administration standards for States and units of local government with responsibility for the administration of Federal elections, and for other purposes." Section 202 of HAVA directs the EAC to serve as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of Federal elections by adopting voluntary voting systems guidelines; by providing for the testing, certification, decertification, and recertification of voting system hardware and software; and by conducting research and activities that promote the effective administration of elections.

In December 2005, the EAC unanimously adopted the 2005 Voluntary Voting System Guidelines (VVSG), which significantly increased security requirements for voting systems and expanded access, including opportunities to vote privately and independently, for individuals with disabilities. The VVSG provide a set of specifications and requirements against which voting systems can be tested to determine if the systems provide all the basic functionality, accessibility, and security capabilities required of these systems. In addition, the VVSG establish evaluation criteria for the national certification of voting systems. As required by HAVA, they also update and augment the 2002 VSSG to address advancements in election practices and computer technologies.

Purpose

Having adopted and published the 2005 VVSG, the EAC considered and approved the development of a set of election management guidelines to complement the technical standards for voting equipment. It is the first time that election administration resources are consolidated into one document and made readily accessible to election

officials at all levels. Before this effort, election officials depended on materials developed and shared almost exclusively at the State and local levels. The National Association of State Election Directors (NASED) has long recognized the need for national guidelines, but it is only now that a Federal agency is able to devote the time and resources needed for the development and distribution of such guidelines. The EAC and NASED have agreed to cooperatively undertake this effort over the next few years.

The creation of the Election Management Guidelines (EMG) is a priority activity under the EAC's national clearinghouse role to promote the effective administration of elections. The long-term goal of the EMG is to provide a comprehensive set of election management guidelines (consolidated into one document) to assist State and local election officials in effectively managing and administering elections. The EAC expects the full set of guidelines to be completed over the next few years. Because of the urgency for resources to assist election officials, however, the EMG have been divided into subject matter modules so that chapters on particular topics can be completed on a priority basis and be distributed to the election community as soon as they are completed. In addition, a series of Quick Start Management Guides has been developed to highlight and summarize information contained in the EMG chapters. They also introduce readers to subject matter modules that will be expanded in future chapters of the EMG.

The EMG subject matter modules cover a wide spectrum of election administration topics ranging from procedures prior to conducting an election to post-election activities and management. Some particular areas to be covered are absentee voting, statewide voter registration systems, voting system management, information technology, precinct definition, poll workers, polling places, military and overseas voters, facility management, office administration, voter outreach, and Election Day procedures and practices. The chapters in this first volume cover information on voting system certification, system security, and physical security.

These guidelines do not endorse one method of election administration over another, and they are not intended as "one size fits all." States and local election jurisdictions are *not* required to consider *or* implement the recommendations or practices contained in the EMG. These guidelines are solely designed to serve as a source of information for election officials and *not* as requirements by which they must abide. Election jurisdictions reserve the right to consider and implement any of the recommendations contained in the EMG in consultation with the appropriate State and local election authorities.

To make the EMG reflective of the realities faced by election officials across the United States, the EAC has sought input and recommendations from State and local election officials and other election professionals and experts who have first-hand experience managing elections. Their input has been invaluable to the development of the EMG. Readers and users of these guidelines are encouraged to provide feedback and recommendations to the EAC regarding the usability and feasibility of the EMG and the practices contained within. The EMG, as a work in progress, can be sustained only by their utility and applicability to the administration of elections.

Comments or questions should be sent to the following:

Mail
U.S. Election Assistance Commission
1225 New York Avenue, NW, Suite 1100
Washington, DC 20005
Attn: Election Management Guidelines

Telephone
202–566–3100
Toll Free: 866–747–1471

Fax
202–566–3127

E-mail
HAVAinfo@eac.gov

Copies of the Election Management Guidelines and the Quick Start Management Guide series are available on the EAC Web site at www.eac.gov or by contacting the EAC at the telephone number or e-mail address listed above.

Chapter 1. Certification

Introduction

The Federal Election Commission (FEC) adopted the first formal set of voluntary Federal standards for computer-based voting systems in January 1990. No national program or organization existed to test and certify such systems to the standards. However, in 1994, the National Association of State Election Directors (NASED) stepped up to fill this void. NASED is an independent, nongovernmental organization of State election officials. This organization formed the Nation's first national program to test and qualify voting systems to the new Federal standards. The organization worked, on a strictly voluntary basis, for more than a decade to help ensure the reliability, consistency, and accuracy of voting systems fielded in the United States. In late 2002, Congress passed the Help America Vote Act of 2002 (HAVA). HAVA created the U.S. Election Assistance Commission (EAC) and assigned to this Commission the responsibility for both setting voting system standards and providing for the testing and certification of voting systems. This mandate represented the first time the Federal government provided for the voluntary testing, certification, and decertification of voting systems nationwide. In response to this HAVA requirement, the EAC developed the Voting System Testing and Certification Program (Certification Program).

HAVA requires that the EAC certify and decertify voting systems. Section 231(a)(1) of HAVA specifically requires the EAC to "… provide for the testing, certification, decertification and recertification of voting system hardware and software by accredited laboratories." The EAC has the sole authority to grant certification or withdraw certification at the Federal level, including the authority to grant, maintain, extend, suspend, and withdraw the right to retain or use any certificates, marks, or other indicators of certification.

Pursuant to the authority granted under HAVA, the EAC has developed and promulgated the EAC Voting System Testing and Certification Program Manual which provides the procedural requirements of the EAC Certification Program. Although participation in the program is voluntary, adherence to the program's procedural requirements is mandatory for participants.

The primary purpose of the EAC Testing and Certification Program Manual is to provide clear procedures to Manufacturers for the testing and certification of voting

systems to specified Federal standards consistent with the requirements of HAVA Section 231(a)(1). The program, however, also serves to do the following:

- Support State certification programs.
- Support local election officials in the areas of acceptance testing and pre-election system verification.
- Increase quality control in voting system manufacturing.
- Increase voter confidence in the use of voting systems.

EAC Testing and Certification Program Manual

The Testing and Certification Program Manual is a comprehensive presentation of the EAC Certification Program. It is intended to establish all of the program's administrative requirements. (The manual may be accessed in its entirety at http://www.eac.gov/docs/Voting%20System%20Testing%20and%20Certification%20Program%20Manual--Final%20--120506.pdf)

The contents of the manual serve as an overview of the program itself and contain the following chapters:

- *Manufacturer Registration*. Manufacturer registration is the process by which voting system Manufacturers make initial contact with the EAC and provide information essential to participate in the EAC Certification Program. Before a Manufacturer of a voting system can submit an application to have a voting system certified by the EAC, the Manufacturer must be registered. This process requires the Manufacturer to provide certain contact information and agree to certain requirements of the Certification Program. After successfully registering, the Manufacturer receives an identification code.

- *When Voting Systems Must Be Submitted for Testing and Certification*. An EAC certification signifies that a voting system has been successfully tested to identified voting system standards adopted by the EAC. Only the EAC can issue a Federal certification. Ultimately, to receive this certification, systems must be submitted for testing and certification under this program. Systems will usually be submitted when (1) they are new to the marketplace, (2) they have never before received an EAC certification, (3) they are modified, or (4) the Manufacturer wishes to test a previously certified system to a different (newer) standard. This chapter also discusses the submission of de minimis changes, which may not require additional testing and certification, and provisional, pre-election emergency modifications, which provide for pre-election, emergency waivers.

- *Certification Testing and Review*. This chapter discusses the procedural requirements for submitting a voting system to the EAC for testing and review. The testing and review process requires an application, employment of an EAC-accredited testing laboratory, and technical analysis of the laboratory test report by the EAC. The result of this process is an Initial Decision on Certification by the Decision Authority, the EAC Executive Director.

- *Grant of Certification*. The grant of certification is the formal process through which the EAC acknowledges that a voting system has successfully completed conformance testing to an appropriate set of standards or guidelines. The grant of certification begins with the Initial Decision on Certification by the Decision Authority. This decision becomes final after the Manufacturer confirms that the final version of the software, which was certified and will be delivered with the certified system, has been subject to a trusted build, placed in an EAC-approved repository, and can be verified using the Manufacturer's system identification tools. After a certification is issued, the Manufacturer is provided a Certificate of Conformance, and relevant information about the system is added to the EAC Web site. Manufacturers with certified voting systems are responsible for ensuring that each system they produce is properly labeled as certified.

- *Denial of Certification*. If the Decision Authority issues an Initial Decision denying certification, the Manufacturer has certain rights and responsibilities. The Manufacturer may request an opportunity to cure the defects identified by the Decision Authority. In addition, the Manufacturer may request that the Decision Authority reconsider the Initial Decision after the Manufacturer has had the opportunity to review the record and submit supporting written materials, data, and the rationale for its position. Finally, in the event reconsideration is denied, the Manufacturer may appeal the decision to the Appeal Authority.

- *Decertification*. Decertification is the process by which the EAC revokes a certification previously granted to a voting system. It is an important part of the Certification Program because it ensures that the program requirements are followed and that certified voting systems fielded for use in Federal elections maintain the same level of quality as those presented for testing. Decertification is a serious matter and will significantly affect Manufacturers, State and local governments, the public, and the administration of elections. As such, the process for Decertification is complex. It is initiated when the EAC receives information that a voting system may not be in compliance with the applicable voting system standards or the procedural requirements of this manual. Upon receipt of such information, the program director may initiate an Informal Inquiry to determine

the credibility of the information. If the information is credible and suggests the system is non-compliant, a Formal Investigation will be initiated. If the Formal Investigation results demonstrate non-compliance, the Manufacturer will be given a Notice of Non-Compliance. Before a Final Decision on Decertification is made, the Manufacturer will have the opportunity to remedy any defects identified in the voting system and present information for consideration by the Decertification Authority. A decertification of a voting system may be appealed in a timely manner.

- *Quality Monitoring Program*. The quality of any product, including a voting system, depends on two specific elements: (1) the design of the product or system and (2) the care and consistency of the manufacturing process. The EAC testing and certification process focuses on voting system design by ensuring that a representative sample of a system meets the technical specifications of the applicable EAC voting system standards. This process, commonly called "type acceptance," determines whether the representative sample submitted for testing meets the requirements. Type acceptance does not explore whether variations in manufacturing may allow production of non-compliant systems. Generally, manufacturing quality is the responsibility of the Manufacturer. After a system is certified, the vendor assumes primary responsibility for compliance of the products produced. This level of compliance is accomplished by the Manufacturer's configuration management and quality control processes. The EAC's Certification Quality Monitoring Program, as outlined in this chapter, however, provides an additional layer of quality control by allowing the EAC to perform manufacturing site reviews, carry out fielded system reviews, and gather information on voting system anomalies from election officials. These additional tools help ensure that voting systems continue to meet the requirements of EAC's voting system standards as the systems are manufactured, delivered, and used in Federal elections. These aspects of the program enable the EAC to independently monitor continued compliance of fielded voting systems.

- *Requests for Interpretations*. A Request for Interpretation is a means by which a registered Manufacturer or Voting System Test Laboratory (VSTL) may seek clarification on a specific EAC voting system standard (VVSG or VSS). An Interpretation is a clarification of the voting system standards and guidance so Manufacturers or VSTL can properly evaluate conformance to it. Suggestions or requests for modifications to the standards are provided by other processes. This chapter outlines the policy, requirements, and procedures for submitting a Request for Interpretation.

- *Release of Certification Program Information*. Manufacturers participating in the Certification Program are required to provide a variety of documents to the EAC. Generally, these documents are releasable to the public. Moreover, in many cases, the information provided is affirmatively published by the EAC. In limited cases, however, documents may not be released if they include trade secrets, confidential commercial information, or personal information. Although the EAC is ultimately responsible for determining which documents Federal law protects from release, Manufacturers must identify the information they believe is protected and ultimately provide substantiation and a legal basis for withholding. This chapter discusses EAC's general policy on the release of information and provides Manufacturers with standards, procedures, and requirements for identifying documents as trade secrets or confidential commercial information.

Program Methodology

The EAC Certification Program is but one part of the overall conformity assessment process; the Certification Program includes companion efforts at the State and local levels.

Federal and State Roles. The process to ensure that voting equipment meets technical requirements is a distributed, cooperative effort by Federal, State, and local officials in the United States. Working with voting equipment Manufacturers, these officials each have unique responsibility for ensuring that the equipment a voter uses on Election Day meets specific requirements.

- The EAC Certification Program has primary responsibility for ensuring that voting systems submitted under this program meet Federal standards established for voting systems.

- State officials are responsible for testing voting systems to ensure that they support the specific requirements of each individual State. States may use EAC VSTLs to perform testing of voting systems that are unique to State requirements while the systems are being tested to Federal standards. The EAC will not, however, certify voting systems to State requirements.

- State or local officials are responsible for making the final purchase choice of voting equipment. They are responsible for deciding which system offers the best fit and total value for their specific State or local jurisdiction.

- State or local officials are also responsible for acceptance testing to ensure that the equipment delivered is identical to the equipment certified at the Federal and State levels, is fully operational, and meets the contractual requirements of the purchase.

- State or local officials should perform pre-election logic and accuracy testing to confirm that equipment is operating properly and is unmodified from its certified state.

Conformity Assessment, Generally. Conformity assessment is a system to ensure that a product or service meets the requirements that apply to it. Many conformity assessment systems exist to protect the quality and ensure compliance with requirements of products and services. All conformity assessment systems attempt to answer the following questions:

- *What specifications are required of an acceptable system?* For voting systems, the EAC VVSG and VSS address this issue. States and local jurisdictions also have supplementing standards.

- *How are systems tested against required specifications?* The EAC Certification Program is a central element of the larger conformity assessment system. The program, as set forth in the manual, provides for the testing and certification of voting systems to identified versions of the VVSG. The Certification Program's purpose is to ensure that State and local jurisdictions receive voting systems that meet the requirements of the VVSG.

- *Are the testing authorities qualified to make an accurate evaluation?* The EAC accredits VSTLs, after the National Institute of Standards and Technology's (NIST) National Voluntary Lab Accreditation Program (NVLAP) has reviewed their technical competence and lab practices, to ensure these test authorities are fully qualified. Furthermore, EAC technical experts review all test reports from accredited laboratories to ensure an accurate and complete evaluation. Many States provide similar reviews of laboratory reports.

- *Will Manufacturers deliver units within manufacturing tolerances to those tested?* The VVSG and this manual require that vendors have appropriate change management and quality control processes to control the quality and configuration of their products. The Certification Program provides mechanisms for the EAC to verify Manufacturer quality processes through field system testing and manufacturing site visits. States have implemented policies for acceptance of delivered units.

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.

Chapter 3. Physical Security

Introduction

In elections, physical security refers to standards, procedures, and actions taken to protect voting systems and related facilities and equipment from natural and environmental hazards, tampering, vandalism, and theft. Physical security safeguards are required for voting systems in storage, in transit, in the polling place, and in use on Election Day through the post-election certified canvass.

Documentation of the election process, from election setup proofing documents to logic and accuracy testing, is the foundation for security in elections. This documentation, required by full-time staff during the pre-election stages and by poll workers on Election Day, provides the audit trail for the election and establishes proof that all components of managing the election were secure at all times. This documentation may also serve as the official court record in the event of a recount or contested election.

This section documents plans, policies, and procedures to manage the various election administration processes and voting system security vulnerabilities. State and county election commissions and municipalities should review these plans, policies, and procedures and consider incorporating them into their local processes.

Conducting a Security Review

One of the most important proactive steps election officials can take is to conduct an election security review. By walking through procedures, performing physical inspections, and considering all aspects of security, including local information systems security practices, possible threats and vulnerabilities can be identified. An election security review identifies key areas where election officials should take steps to ensure the security and integrity of election administration.

The following activities should be part of an election security review:

- Review overall policies to ensure proper separation of job duties throughout the election administration process.
- Perform an election administration risk assessment. Identify potential opportunities in the election administration process where election security and integrity is vulnerable to destruction, disruption, tampering, or corruption from

internal or external sources. Examples include building fire, power failure, after-hours theft, malfunctioning sprinkler system, misprinted ballots, paper ballots counted twice, bomb scares or terrorist acts, failure of election boards to report for duty, disruptions by voters or poll agents, and so forth. List the potential security exposure and the impact on the election from each threat. Consider whether the likelihood of each threat is high, medium, or low, and develop plans to mitigate or eliminate each threat starting with those considered high.

- Review the audit trail from the last election in its entirety. Analyze whether sufficient documentation exists to validate the integrity of the election.
- Conduct a debriefing to identify lessons learned about issues and problems encountered in previous elections. This activity should become a regular part of closing out each and every election.
- Inventory the list of procedures used throughout the election administration process. Evaluate each procedure to determine whether it needs to be updated based on the security review.
- Evaluate the security of the computer systems used in election administration by conducting an information systems security assessment.
- Perform a physical security review to assess access and controls of all office and storage facilities used in the election administration process. Consider the relative security of other agencies sharing the facilities. Evaluate disaster recovery, terrorism, and weather-related considerations, and develop a plan to mitigate such risks. Also consider involving local or State law enforcement agencies.

At no point in the security review allow a person to validate their own security procedures and functions. Use the two-person accountability principle and have the procedures reviewed by someone other than the person who does the work. This objectivity will enhance faith in the integrity and honesty of the review.

Engage County and Municipal IT Staff. Elections are, at their core, an information system comprised of processes, people, technology, and data. Engage county and municipal IT staff or local community college or technical school staff to assist in the security review and to help establish and implement applicable election management system security measures. They should be familiar with many of the vulnerabilities and risk management steps related to information systems and can be of valuable assistance. Include county or municipal IT staff or local community college or technical school staff early on in the process and on a continuing basis.

Review Equipment Storage, Logistics, and Maintenance. The election administration security risks associated with voting systems equipment go beyond the obvious concerns of theft and destruction. Everything from building security, access control, and configuration management of the voting system equipment is an important component in the overall election security.

- Perform a physical security review to assess access and controls of the facility in which the voting systems equipment is stored and maintained. Maintain a key control list of all personnel with keys and access to the facilities. Maintain an access log including sign in and sign out dates and times of all personnel, including visitors.
- Implement two-person integrity security measures when setting up the voting system equipment for an election. Never allow a voting system vendor or employee to have uncontrolled access of county election equipment storage and maintenance facilities.
- Take into consideration long-term storage and security needs when designing storage and workspace.
- Implement an effective asset management and inventory control system for all components of the voting system. Consider testing procedures and sign off on all equipment returned from the vendor after maintenance to ensure proper versions of the equipment hardware, software, and firmware.
- Nongovernment officials should never be allowed to have unattended or unmonitored access to stored voting equipment. Government election officials should be responsible for maintaining the access log and supervising the activity.

Steps to take when conducting an election security review:

- Create or update the master election audit trail checklist to ensure it identifies all required audit trail documents for an election.
- Review all election audit trail checklists to ensure they incorporate two-person integrity security measures such as dual sign-off.
- Review election commission work areas to ensure office space is appropriately isolated and undetected access by unauthorized individuals is not possible.
- Review voting equipment storage and work areas to ensure only authorized personnel have access.

- Review the list of personnel who have keys to election office work areas and voting equipment storage to ensure all keys are accounted for and only authorized personnel have keys. Eliminate the distribution of master keys or key cards. Instead, issue access keys or key cards to personnel based on job duties and responsibilities, ensuring that individual staff members do not have the ability to enter the office and access the voting system undetected.

- Review chain-of-custody procedures, the use of tamper-evident seals, and inventory control/asset management processes to ensure voting units and associated equipment are properly and securely controlled and are accounted for throughout the election administration process.

Steps to follow for reviewing equipment storage, logistics, maintenance, and security procedures:

- Ensure physical, tamper-evident seals are employed throughout the election administration process.
- Review storage and maintenance facility property insurance to ensure coverage is appropriate and adequate.
- Review inventory control/asset management processes.
- Create or update appropriate procedures to ensure absentee and emergency ballot blank paper stock are controlled at all times.
- Review other facilities shared with voting equipment storage, logistics, and maintenance for potential security vulnerabilities.
- Develop physical security procedures and safeguards to document the controlled physical access to voting systems and the facility or facilities where they are housed.
- Document all security related repairs and modifications to the physical components of the facility where voting systems are stored (i.e., walls, doors, locks, cameras, alarm systems, etc.).

Security—Personnel

Another important factor in determining the vulnerability of a system is the people involved; it is they who must implement security policies and procedures and defend against any attacks.

- Qualification guidelines should be established for choosing the person(s) for operating and administrating (creating databases, defining ballots, testing, and maintaining equipment) the voting system.
- Perform background checks on election officials authorized to define and configure elections and maintain voting devices to minimize the risk of election tampering.
- Custodians of voting machines must be fully competent, thoroughly trained, and sworn to perform their duties honestly and faithfully.
- Develop a detailed "Rules of Security Behavior" sign-off sheet for all levels of personnel responsible for using the voting system (election director, chief judges, poll workers, rovers, field technicians, etc.) and maintain a copy of the signed forms on file.
- Establish policies and procedures for visitors and observers. At minimum, these procedures should include employee-monitored entrances and exits with a sign-in/sign-out log and issuance of a numbered visitor badge to be worn at all times.

To effectively manage a polling location on Election Day, establish the number of personnel needed and their duties.

- Maintain separation of duties for poll managers to provide "checks and balances" during the election process.
- Incorporate two-person integrity security measures to polling place procedures.
- Provide adequate security of election equipment at the polling place at all times.

Security—Paper Ballots

Protecting the security of paper ballots is also a component of providing physical security. Election administrators should have a documented plan in place to provide for the management of optical scan or paper ballots, ballot-on-demand ballots, and all ballot stock. This plan should include details pertaining to the audit trail and chain of custody for the ballots with strict control over the ballots and ballot stock at all time.

- The security of paper ballots includes security in the election office facility and at the polling place on Election Day. At least two election officials should oversee all processes, including the transfer of ballots and other election materials from the polling place to the central office.

- Two or more staff members should receive the ballot order and verify the accuracy and quantity of ballots against the ballot order request. Once validated, the ballots should be stored in a secure building with restricted access in a secure area.

- Ballot-on-demand is often used to supplement printed ballot stock. If used, election officials should implement internal controls to safeguard ballot stock from fraudulent or inappropriate use. For example:

  - Two or more election officials should monitor, record, and balance daily ballot-on-demand activity.

  - Election officials should reconcile the number of blank ballots received from the vendor, the number printed or spoiled, and the number of unused ballots.

Security—Voting Equipment and Peripheral Devices

Voting Equipment Storage (Warehousing/Staging Facility) and Inventory Control

Physical security of all voting system equipment and peripheral devices must be maintained at all times. The security measures should include the following:

- Maintain complete and accurate inventory of all voting system equipment. This includes voting devices, optical scanners, communication equipment, supervisor or administrator devices, ballot activation devices, and storage media.

- Assign personnel the responsibility of maintaining accurate inventory.

- Provide physical access control to the storage facility only to authorized personnel. Following is a list of recommendations:

  - Make sure all personnel have signed security agreements on file.

  - Each staff member should be issued a unique code for entry and exit tracking. Staff members should wear identification badges at all times.

  - All visitors, vendors, and maintenance personnel should be authenticated through the use of appointments and identification checks in order to gain access to the voting system equipment.

- If video cameras are used, schedule regular checks to verify they are fully operational.

- Change keys or combinations on locks as necessary for each election.

It is recommended that the following information regarding the voting system equipment be tracked:

- Equipment—Maintain a list of equipment, serial numbers, and quantity in the storage facility.
- Machine Checkout—Maintain a list of voting system equipment that has been released from the storage facility.
- Usage History—Maintain a history of elections for which each voting device has been used.
- Repair History—Maintain a history of repairs to individual voting devices.

Inventory control should consist of tracking the voting system equipment when it is being—

- Released and returned for any official election.
- Released and returned for any demonstration of an election.
- Accepted from or returned to the vendor (including warranty and maintenance repairs).

A barcoding system should be explored as a method for tracking the location of voting system equipment. All electronic media, regardless of type (memory packs, compact flash cards, PCMCIA (Personal Computer Memory Card International Association) cards, voter card encoders, supervisor cards, and key cards) should be *permanently* identified with a unique serial number. The serial numbers should be recorded as part of the internal inventory audit trail.

A "Voting Equipment Delivery Sheet" should be used to record and track equipment delivery information, description of equipment (including serial numbers), and signatures of equipment handlers or recipients.

Voting Equipment Storage (Warehousing/Staging Facility)—Access Control

- Voting devices must be kept in a locked (secured) facility.
- Access to the storage facility should be restricted to only authorized personnel. Access should be restricted through the use of badges, door entry access devices, and monitoring systems. The best method of access control is one that uniquely identifies the person, authorizes entry, and logs the date and time of access.

- The storage facility should be equipped with monitored security and fire alarm protection.
- For additional security, the facility could be monitored by video cameras.

Consider the following questions:

- What procedures are in place to assure the physical security of voting machines and paper ballots before an election?
- How and where are equipment, ballots, and ballot stock stored? How is the facility secured against theft, tampering, and vandalism?
- What protections are in place to assure access is permitted only for authorized personnel?
- Who installs equipment upgrades, a county official or a vendor?
- Do vendors ever handle any voting equipment?
- If vendors are allowed to handle voting equipment pre-election, are county officials required to be present?
- Has the physical security of the voting equipment, ballots, and other election material been protected against terrorism and other "Homeland Security" issues?

Security—Election Process

Securing the Voting Devices During Preparation and Transport to Precinct

- The voting devices should be secured with tamper-proof numbered seals. Access to the voting devices' power control and election results storage media should be secured (controlled) within the voting device. The serial number of all seals should be recorded for verification during precinct setup.
- It is recommended that for each voting device, records are kept of the following:
  - The serial number of the voting device.
  - The serial number of all seals used to secure the voting device for delivery.
  - The number registered on the protective counter.
  - The serial number of the seal used to secure the voting device after the polls have closed.

- Develop an operational plan defining what will be delivered, where, by whom, and when. Use delivery sheets to keep track of the exact polling place each voting device is delivered to.
- It is strongly recommended that the auxiliary voting equipment and supplies (ballot activation devices, administrator devices, communication equipment, seals for poll closing, etc.) remain in the possession of election officials until the opening of the polls on Election Day. If the voting devices are delivered to the polling location before Election Day, they must be secured at the polling location (e.g., cabled together and locked or secured in a locked room). Any other voting equipment or supplies should also be secured. Designated poll manager(s) should verify receipt and sign-off on the delivery of voting devices and necessary election supplies (ballot activation devices, administrator devices, communication equipment, closing seals, etc).
- Voting systems should be moved in a controlled transportation mode. In other words, they are locked and sealed in any vehicle or container at the beginning of the transportation and unsealed at the delivery point. Sealing and unsealing should be logged and completed only by election officials.

Consider the following questions:

- Are voting equipment and ballots transported to polling places by county officials or poll workers?
- How and when are voting equipment and ballots transported to the polling places?
- If poll workers transport voting equipment and ballots, when do they receive the equipment and ballots? If poll workers receive the voting equipment and ballots significantly in advance of the election, how and where are the materials stored until the election?
- Are detailed logs kept of who takes custody of equipment and ballots and those person(s) contact information?
- How are voting equipment and ballots secured from tampering from the time they leave election office custody to the time they are delivered to the polling places?
- Are serial numbers or other secure, tamper-proof devices or seals placed on all ports where memory cards are inserted?

Securing the Voting Devices During Walk-In Absentee/Early Voting

- Walk-in absentee voting devices should be prepared, tested, delivered, and set-up in the same manner as voting devices used on Election Day.
- The same walk-in absentee voting storage media should be placed in the same voting device every morning and removed every night.
- The voting storage media should be secured each night in a tamper-proof location, preferably within the election office.
- Voting devices should be closed, sealed, and secured at the end of each day. The number on all protective seals and public counters should be recorded. In addition, seals and counters should be verified before the voting devices are used for voting the next morning.

Securing the Voting Devices During Mobile Absentee/Early Voting

- Mobile absentee voting devices should be prepared, tested, delivered, and set up in the same manner as voting devices used on Election Day.
- Voting devices should be closed, sealed, and secured at the end of each day. The number on all protective seals and public counters should be recorded. In addition, seals and counters should be verified before the voting devices are used for voting the next morning.
- The mobile unit containing all voting devices should be returned to the Election Office every evening and stored within a secured facility.

Securing the Voting Devices on Election Day—Precinct Setup

- If voting devices and election supplies are delivered to the polling place by anyone other than poll managers, the poll manager(s) should verify the serial numbers of all voting devices and necessary election supplies (ballot activation devices, administrator devices, communication equipment, closing seals, etc.).
- Designated poll managers should verify voting device numbers and the numbers of all seals and tamper-resistant tape on all voting devices and inspect the voting devices for evidence of tampering. This should be a two-person integrity security process and all poll managers should sign-off on this validation.
- Voting devices setup should be as follows:
    - Access to the voting devices' power control, counter controls, and election results storage media must be controlled within the voting device and inaccessible to the voter.

- Voting devices exterior should be in plain view of the poll managers at all times.

- Poll managers should maintain control of all administrator and ballot activation devices.

Consider the following questions:

- How are poll workers trained to be alert for signs of pre-election tampering?
- How are poll workers trained to respond if tampering is suspected or discovered?

Securing the Voting Devices on Election Day—Opening the Polls

- Poll managers should activate each voting device, including the following:
  - Verify date and time and precinct on the voting devices.
  - Verify the protective seals and public counters on the voting devices.
  - Verify that the electronic paper audit trail is functioning.
- Poll managers should secure administrator devices and communication equipment during the day.
- The poll manager and all poll workers should sign-off on a checklist to verify all opening procedures were followed.

Securing the Voting Devices on Election Day—Voting

- The area around the voting devices must be secure at all times. Only poll managers, legally authorized personnel, and registered voters should be allowed in the voting device area. A voter should not be allowed to enter this area until a voting device is available for his or her use.
- Each poll worker should have a clearly defined role so voters are able to clearly identify them and their particular responsibilities as they move through the polling place.
- Provisional voters should be directed to a separate check-in table or area. This assures that provisional ballots are handled uniformly and also establishes ballot accountability for auditing purposes.
- The poll manager must maintain control of the ballot style identification device (card, slip, tag, label, ticket) and the ballot activation device.

- Poll managers should periodically inspect the voting devices for any damage or tampering and to ensure the device is powered by electricity.
- Poll managers should perform periodic verification of the number of voters processed to the number of votes recorded (public counter) on the voting devices and balance that number to the total number of signatures in the poll book.

Consider the following questions:

- Are poll workers trained to ensure that voter lines form at the registration table and not at the voting devices, especially during periods of heavy volume?
- Are poll workers trained to issue a voting activation card to a voter only when a voting station is available for use?
- Are "troubleshooters" available to visit and roam polling places on Election Day to provide support to poll workers?

Securing the Voting Devices on Election Day—Poll Closing

- Poll managers should validate that the number of ballot activation devices and voter activation cards issued to the polling place are collected and secured in a transport case for return to the local election office.
- The voting devices should be secured using the numbered "closing" seal. The signed affidavit should be returned by a poll manager to the local election office with the number of the closing seal, number voting devices, number of the public and protective counter, and the voting precinct recorded on the envelope.

Securing the Voting Devices During Tallying

- At the end of the day, print out end-of-day vote totals from each individual voting device and deliver the printed tapes to the local election office in a secure manner.
- The election result storage media from all voting devices within the polling location should be accounted for and reconciled.
- The election result storage media and printed tape(s) should be secured in a numbered, sealed pouch and transported from the polling place to the local election office or designated collection point.
- If transmitting unofficial election results by modem, (1) print end-of-day vote totals from each device, (2) limit access control to the telecommunication

devices, (3) enable modem access only when uploads are expected, and (4) apply sufficient encryption and verification of data to protect the transmission of vote tallies.

- Establish procedures to securely transport election results from optical scanners to vote tabulation computers if the optical scanners are located in a different location from where the vote tabulation takes place.

Security the Voting Devices During Tabulation at the Election Office

- Election officials should perform a verification of results transmitted by modem to the county election office through a separate count of the election result storage media containing the original votes cast.

- The offices where the vote tabulation is being conducted must be secure. Do not allow unauthorized and unescorted personnel to be in contact with the tabulation equipment. Only authorized election officials should be allowed in the tabulation equipment room.

- Consider the use of video monitoring to secure the vote tabulation area.

- Consider uniformed security or police officers to secure the ballot room and voting equipment.

Consider the following questions:

- Are all paper ballots and electronic election media in the possession of at least two election officials or poll workers (using the two-person accountability principle) during its transport to the central or remote count locations?

- Is the election tabulation process secure by protecting the premises where the vote tabulation is being conducted? Are unauthorized and unescorted personnel allowed to be in contact with the tabulation equipment?

- What physical security measures have been implemented for the room containing the computer running the tabulation software?

- Are printed result tapes and a backup copy of the tabulations in locked storage in a secure location?

- Is there a complete chain of custody with two-person integrity security measures for all election materials?

Securing the Voting Devices During Transport to Storage

- Only designated personnel should transport voting devices to the local storage facility. Custodians of the voting devices should verify receipt of all devices, confirm that the devices have not been tampered with during transport, and sign-off on the receipt of the voting devices.

- Only designated personnel should transport election supplies (administrator devices, ballot activation devices, communication equipment, etc.) to the local election office. A local election official should verify receipt and sign-off on the delivery of the election supplies.

Securing the Voting Devices During Storage and Post-Election

- Local election officials should maintain an inventory of election materials. These materials should be securely stored until the period of election protest and appeals has ended.

  Election materials include the following:

  - Voting devices (including memory cards where applicable).
  - Administrator and ballot activation devices.
  - Seal envelopes.
  - Voter registration (poll) lists.
  - Election result tapes and printouts.
  - Field supervisor and rover reports.
  - Poll worker daily logs.
  - Reconciliation reports.
  - Audit data (includes retention of the completed master election audit trail checklist mentioned on page 16.
  - Voting Equipment Delivery Sheets (mentioned on page 29).

- Two copies of the inventory list should exist; one list should remain stored with the election materials and one list should be kept at the local election office. The local election official should verify and sign the inventory list.