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.