pennsylvania
DEPARTMENT OF STATE

September, 2016

GUIDANCE ON ELECTRONIC VOTING SYSTEM PREPARATION AND SECURITY

As a reminder for counties, and refresher on good cyber hygiene practices, DOS recommends the following procedures in the preparation and configuration of election management software and precinct voting systems to better ensure security. Counties may wish to contact their own IT Department to review these procedures. The Department recognizes that resources vary among counties, but encourages all counties to follow these procedures as closely as possible. ***If a county uses an outside vendor to perform any of the election preparation tasks, the Department strongly recommends that the vendor follow these procedures as closely as possible.*** Should county election administrators have questions regarding the following recommendations, they should contact the Department through Jessica Mathis 717-772-4507.

A. NETWORKS

Isolate networks involved in any part of the election operation.

1. Map or inventory your networks.

Security begins with knowing what is connected to each of your networks. To identify the existence of authorized and unauthorized devices and lost or stolen assets, begin with an inventory.

- □ Develop an inventory of all devices connected to or running on your network, including devices that have been or will be only temporarily connected. The list of devices should include all computers, laptops, tablets, smart phones, PDAs, thumb drives, removable hard drives, printers, routers, switches, and servers.
- □ For each device, document the type of device, its location, its assigned owner and its history of connection to the internet.
- □ Verify that no default passwords are used on any devices, including routers, and that all passwords are appropriately complex and secured.
- □ Review the inventory with executive staff at least yearly, reconcile any discrepancies and discuss the security of the assets.

2. Isolate the computers involved in elections from internet-facing networks.

Use the system inventory to ensure that all computer systems that are involved in the canvass of the election are physically isolated from the internet. If a portion of your system is not yet isolated, it must be isolated immediately and all components of the system must remain isolated as long as they are used in any part of the canvass process. These systems include computers that:

- run election management software;
- store the prime copies of software/firmware used in the election;
- initialize voting system firmware;
- create ballot definition files;
- initialize and write to the removable media that are inserted into precinct voting machines; or
- record and aggregate vote tallies from precinct voting machines' removable media.

For each of the computers listed above, verify that no pathway exists to an internet-facing network router. Where necessary, disconnect components to ensure that there is no path between a system that deals with sensitive functions or information and the internet. To fully disconnect, it may be necessary to physically unplug device(s) from a network.

3. Monitor connections, especially temporary connections.

Connections to the isolated network must be strictly monitored. Transfer data in and out of the isolated network using only clean media, preferably write-once media such as CD-R or DVD-R.

Implement procedures to prevent any prohibited connections to the isolated network, including the following types of connections:

- □ wireless network connections, such as Wi-Fi and Bluetooth;
- □ any device with an internet connection, or any device that has ever been connected to the internet;
- □ USB drives;
- □ smart phones;
- □ hotspots;
- □ email;
- □ video or music streaming;
- □ web access;
- □ VPN;
- □ teleconferencing service;
- □ message service; or
- □ software updates or database updates delivered over a network or from online sources.

B. BACKUPS

Any critical data involving elections should be frequently backed up, and the backups should be stored on media not connected to the internet. Backups should not be overwritten, but instead retained and new backups created. Instead of incremental backups, back up critical data frequently and in full to retain the ability to roll back to clean copies of important data in the event of a breach. Backups should be tested to ensure that recovery is possible.

C. PASSWORD AND PERMISSIONS MANAGEMENT

Many breaches occur because the administrator and/or guest default passwords are not regularly changed and are readily known by attackers, or because some users have inappropriate privileges. Without changes, the standard configurations that come installed by default on most computers and servers are not secure. Configuring devices using a few simple and easy steps can reduce the risk of compromise.

1. Change default credentials and avoid "shared" credentials.

☐ Ensure default passwords are changed (especially for new systems or devices).
☐ Require all users to create strong passwords that combine upper and lower case letters, numbers, and special characters for access to all systems and are an appropriate length, e.g. 8-12 characters.
☐ Audit existing systems and change any default passwords where found.
☐ Ensure passwords and accounts are unique and not shared among multiple users.
☐ Ensure business partners are following correct processes, because shared credentials have led to breaches at third parties.
☐ Require passwords to be changed if a system is compromised or an administrator with high level privileges leaves employment.
☐ Inventory all user accounts and delete any accounts that are no longer valid.

2. Restrict administrative access and monitor privileged users.

☐ Practice the principle of "least privilege" and do not allow anyone access to the canvass system or its data unless business needs specifically require access. Restrict users from having more privileges than they need. By the same token, at least two users should have access to administrative functions that are password protected in case one person becomes unavailable.
☐ Check each user's current privilege level and change privileges as appropriate.
☐ Ensure administrative accounts and elevated privileges are locked down and only used when absolutely necessary (i.e., administrator privileges should only be used while performing administrator duties).

- □ Where necessary, enforce the use of separate accounts with differing access levels to limit the potential for accidental or malicious data exposure.
- □ Limit and manage those who have administrative privileges to change, bypass, or override your security settings.
- □ Restrict both physical and network user access.
- □ Ensure that privileged users understand the policies and expectations.
- □ Set up automatic logging of privileged use, as well as procedures for saving and tracking logs.
- □ Set up automatic alerts and alarms triggered by unplanned privileged use, and investigate any such alerts and alarms.
- □ Delete the account of any user who leaves the employment of either the department or the county. All passwords should be changed immediately after an employee departs.

D. VOTING SYSTEM PREPARATION

The steps listed below, if followed, can minimize the risk of introduction of any malware or error into the precinct voting systems.

1. Portable storage media, e.g. USB drives, PCMCIA cards, or other media used to transfer files between the EMS and the voting system, should be brand new. Alternatively, removable media that is being reused should be reinitialized, e.g. reformatted, before using in each election.

2. After media containing the ballot definition files are loaded into the machines, the ports containing the media should be sealed with tamper-evident seals.

3. The tamper-evident seals should be numbered and the county should record the numbers of the seals with the serial number of the system. Counties should train poll workers to identify a broken seal and report it. Any machine with a broken seal should not be used in the election.

4. Conduct thorough pre-election testing that is open and transparent. Notify local party officials and advocacy groups about the date, time and location of your testing. *See* “Logic and Accuracy Testing Checklist,” below.

5. Counties should maintain a robust chain of custody protocol that documents access to all components of the system including the county computers and the warehouse storing the voting systems. Counties should keep a record of all electronic devices and media that includes the date and time voting system devices and media were given to poll workers and the date and time that the components were returned to the county.

6. After counties deliver voting systems to the polling place, the voting systems should be stored in a locked location with limited access, not in a public area that would allow anyone to be alone with the machines.

E. UNOFFICIAL CANVASS ON ELECTION NIGHT

☐ No results from precinct voting systems should be transmitted electronically, either over a network connection or via modem.

☐ Media should be removed and physically transferred to the county by two poll workers who travel together in accordance with the Election Code (or by other secure means already in place).

☐ The computer system that aggregates results should not be connected to any network.

☐ Vote totals should be written to disk and manually walked over to the server that hosts the county website.

☐ If results are transferred to the website multiple times, counties should use a clean disk for each transfer so that malware from the internet-facing device is not introduced into the isolated network.

F. FILE TRANSFER FROM VENDORS

Many high profile breaches have been the result of a third party provider being targeted by hackers to access the company data or network. Business partners or vendors need to be held to the same stringent controls. This guidance applies to any vendor that is providing technical support to the counties for any component of the system involved in the canvass of the election.

If a county uses an outside vendor to develop, create, or prepare any of the files that are loaded into the election management software or voting systems, the transfer of those files must be as secure as possible.

The vendor should send the files on clean, write-once media, created on an isolated network that is password protected and the password should be communicated in a separate transmission. Alternatively, if the vendor plans to electronically transfer the files, the vendor should use a secure file transfer protocol (SFTP) site. The file should be encrypted ("hashed") on the vendor's side and the county side. Ideally, a representative of the vendor and a representative of the county should be in communication with each other via telephone during the transmission. If the file does not "hash" correctly on the county side, the county should notify DOS immediately. The system receiving the file should not otherwise be used in the canvass process. The county should manually transfer the files to its canvass system using the practices outlined above. *See* network isolation section above.

PRE-ELECTION LOGIC & ACCURACY TESTING CHECKLIST

Primary Purposes of Pre-election Testing:

1. Verifying that the election is correctly defined.
2. Verifying that the voting systems are properly programmed.
3. Verifying that all accompanying hardware is in working order.

Testing Prerequisites:

- □ Advertise the dates, times and location of pre-election logic and accuracy (L& A) testing. Notify interested political parties and advocacy groups of the testing.
- □ Proofread balloting materials at all stages of setup and production. Use more than one proofreader, if at all possible.
- □ Ensure that you have adequate staff to conduct public testing.
- □ Ensure that you have adequate space to conduct public testing.
- □ Prepare test decks/test scenarios for use during L & A testing.
    - o Prepare test decks/test scenarios for all of your ballot configurations.
    - o Prepare test decks/test scenarios that include votes for all candidates and ballot questions.
- □ Test every hardware component of the voting system(s), including scanners, touch screens, printers, memory cards, electronic poll books (if applicable), voting booths, etc.
    - o Check the batteries in voting systems that use batteries as either the primary power source or as backup to the primary power source.
    - o Implement a process to ensure that all batteries are fully charged for Election Day.
    - o Check the scanner heads on optical scanners.
    - o Check the calibration of scanners.
    - o Verify the calibration of DRE touch screens and replace or repair as needed.
- □ Verify the date and time settings on all voting systems.

Conducting L & A Testing:

- ☐ Use pre-election auditing checklists to ensure that each step of L & A testing is completed, that the memory card is zeroed out, and the voting machine mode is set for Election Day.
- ☐ Set each voting machine to be tested in "Election Mode" rather than "Test Mode."
- ☐ Whether you are conducting manual or automated L & A on Direct Recording Electronic (DRE) voting systems, test all ballot configurations.
- ☐ Prepare test decks for optical scan machines, and test scenarios for DRE machines, that include test ballots for straight-party voting, overvotes, undervotes, blank ballots, and write-in votes.
- ☐ Confirm that all error messages properly display.
- ☐ Ensure that some of the optical scan test ballots are marked by hand.
- ☐ Test precinct-level scanners using the memory cards specific to those locations on Election Day.
- ☐ Review the audio set up of ballots.
- ☐ Test the central tabulation software by loading and generating summary reports of all test votes.
- ☐ Document testing results as you would official results.
- ☐ Retain and seal all pre-election testing materials.