Onondaga County Board of Elections

Meeting Agenda

July 31, 2025

2:30 PM

Type of Meeting: Decision Making

Commissioners: Dustin Czarny and Kevin Ryan

Invitees: Nicole Walsh, Dez LaFave, Michelle Edinger, Sydney Szczesniak

I. Call to Order: Dustin Czarny at 2:31

II. Roll Call: Dustin Czarny, Kevin Ryan, Nicole Walsh, Michelle Edinger, Sydney Szczesniak

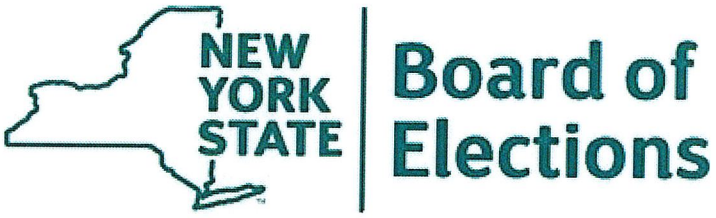
III. Approval of Agenda: 2 YES / 0 NO

IV. New Business:

1. Approval of USB Policy Plan 2 YES / 0 NO
2. Approval of 14-character passwords for staff 2 YES / 0 NO
3. Approval of Absentee Ballot Policy 2 YES / 0 NO
4. Approval of Social Media Calendar 2 YES / 0 NO
5. Approval of Village Election Costs 2 YES / 0 NO
6. Approval of Contingency Plan 2 YES / 0 NO

V. Adjournment: 2:40pm / Kevin Ryan second

Recommendations and Best Practices for Removable Media and Data Transfers



40 North Pearl St., Suite 5

Albany, NY 12207

January 9, 2019

Version 1.0

Version History

Version: Date	Description	Updated By
1.0: 1/9/2019	Initial publication of Recommendations and Best Practices for Removable Media and Data Transfers. Document provides suggestions, recommendations and best practices that County Board of Elections should adopt and implement to increase the security of election operations during the election process.	Election Operations

Contents

Purpose

This document provides suggestions, recommendations and best practices that County Board of Elections (CBOE) should adopt and implement to increase the security posture of election operations during the election process. This document will be reviewed and updated based on the changing election environment, industry standards and cyber security threats. County Board of Elections should make every effort to implement the guidance provided in this document.

Overview

The use of removable media and performing data transfers play an integral part in election processes. Removable media is used in transferring data from election management systems (EMS), precinct based optical scanners (PBOS), central count optical scanners (CCOS), ballot marking devices (BMD), automated audit tools, desktops, laptops, election night reporting activities as well as numerous every day election activities. Each CBOE should ensure that removable media are free from viruses and malware before being used in any device.

The New York State Board of Elections (SBOE) has certified a closed network configuration for county board of elections to implement. A closed network is a stand-alone Local Area Network (LAN) that is restricted (closed) in that it only connects to an EMS server or servers, central count voting system or automated audit tool to specific workstations within a CBOE local and controlled environment, typically a room or building. The closed network is restricted to specific workstations and users and not connected to any other internal or external network. Removable media must be introduced into this closed network in order to transfer election configuration information to PBOSs, CCOSs, BMDs, automated audit tools and to receive election results from the same systems. The use of removable media within a closed network must be strictly controlled so as not to introduce viruses or malware.

Additionally, election night reporting (ENR) is a process performed by each CBOE. Beginning at 10 p.m. on Election Night, each CBOE must upload their first XML file containing unofficial election results to the SBOE and for posting to the County's website. Unofficial election results may be generated from a closed network EMS, transferred to removable media and then uploaded by the CBOE via NYSVoter VPN connection to SBOE. The use of removable media may introduce viruses and malware that may potentially change unofficial election results. Election night reporting is not only critical to informing the public but also assuring the public that the election process is fair, honest and transparent. Erroneous reporting undermines the trust of the public to the entire election processing.

The use of removable media is necessary to carry out New York State's election processes. Insecure methods of results/data transfer increase the risk of compromising the integrity and

confidentiality of the election data. This document will provide recommendations to reduce risks in using removable media in New York State's election processes.

Definitions

The following terms will be used in the recommendations provided.

CD-R: a blank compact disc which can only be recorded on once (write-once media).

Closed Network: a stand-alone Local Area Network (LAN) that is restricted (closed) in that it only connects an EMS server or servers, central count voting system or automated audit tool to specific workstations within a CBOE local and controlled environment, typically a room or building. The closed network is restricted to specific workstations and users and not connected to any other internal or external network/internet. A standalone EMS system that is self-contained can also be considered a closed network.

Dedicated USB Flash Drive: a data storage device which is used for a single purpose throughout the lifecycle of the device.

- *Election Night Reporting (ENR) USB Flash Drive*: only purpose is to transfer unofficial results from the EMS closed network to NYSVoter VPN open network.
- *Ballot PDF Transfer USB Flash Drive*: only purpose is to transfer ballot PDFs from the EMS closed network to a PC connected on the CBOE open network.
- *Bridge Data USB Flash Drive*: only purpose is to transfer bridge data files from a PC connected on the CBOE open network to the EMS closed network.
- *Data Import USB Flash Drive*: only purpose is to transfer data import files from a PC connected on the CBOE open network to the EMS closed network.

DVD-R: a digital versatile disc recordable which can only be recorded on once (write-once media).

Encryption: A technique used to protect the confidentiality of information. The process transforms ("encrypts") readable information into unintelligible text through an algorithm and associated cryptographic key(s).

Encryption is a cryptographic operation that is used to enhance security and protect the State's electronic data ("data") by transforming readable information ("plaintext") into unintelligible information ("ciphertext"). Encryption is an effective tool in mitigating the threat of unauthorized access to data (NYS-S14-007).

Erase: for purposes of this document, erase is synonymous with the definition of clear as defined in NIST 800-88 R1 – Guidelines for Media Sanitization.

Open Network: a Wide Area Network (WAN) that is an open network (connected to an external network/internet).

Removable Media: Portable data storage medium that can be added to or removed from a computing device or network. Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD). Source – CNSSI 4009-2015

Write blocker: a device that allows acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents by allowing read commands to pass but by blocking write commands.

General Recommendations

1. All removable media that are used in the voting process are considered part of the voting system and must always be physically secured (that is, in use or locked away) and only used for the voting process.

2. All new removable media must be sanitized before use in any CBOE device. For all other existing removable media, if there is any uncertainty in the status, removable media must be sanitized before use in any CBOE device. Removable media must be sanitized per NYS ITS IT Standard: Sanitization/Secure Disposal (NYS-S13-003).

3. For removable media that will be used on board of elections closed network, a write blocker should be used anytime said removable media is used on a device that is not connected to the EMS closed network.

4. For removable media that has been used outside the EMS closed network without a write blocker, or if you are unsure of usage, the removable media cannot be used in the EMS closed network environment until the removable media has been sanitized. Removable media must be sanitized per NYS ITS IT Standard: Sanitization/Secure Disposal (NYS-S13-003).

5. For EMS, CCOS, PBOS, BMD, and automated audit tools, system upgrades must be distributed via write-once media (CD-R/DVD-R) and hash checked before installation.

    a. For bridge data, downloaded files must be scanned with anti-virus and anti-malware software. If no threats are found, the files may be written to write-once media (CD-R/DVD-R) or to the dedicated bridge data USB flash drive that will be used to update the EMS database on the closed network. Once the database is updated, the data

must be manually verified by a defined process and procedure to ensure the integrity and accuracy.

Best Practices for Transmission of Files and Data

Election activities create the need to transfer files and data on a regular basis. CBOEs must ensure that the transfer of files and data is handled in a most secure method. Below are best practices that should be followed when transferring files and data for election activities.

1. **Secure file transfer options**:
    a. Secure File Transfer Protocol (SFTP) – network protocol that provides file access, transfer and management using Secure Shell (SSH) when transferring files between a client and server over a network. SSH is a cryptographic network protocol that provides the secure channel by encrypting both the commands and data during the session.
    b. FTPS (also known as FTPES, FTP-SSL, S-FTP and FTP Secure) – file transfer protocol that adds support for Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cryptographic protocols.
    c. Hypertext Transfer Protocol (HTTP) for Secure Communication (HTTPS) – communication protocol that implements Transport Layer Security.

    Note: the use of File Transfer Protocol (FTP) is not recommended as it does not provide a secure channel in the transfer and management of files between a client and server (sender and recipient).

2. **Encryption in Transit**:
    Encryption in transit should be used to protect files and data from being accessed by unauthorized users. Encryption enables the security principal of confidentiality to be maintained. The need for encryption of information is based on its classification, risk assessment results, and use cases.

    Per NYS ITS IT Standard: Encryption (NYS-S14-007), Encryption is required for data in transit in the following situations:

    1. When electronic Personal, Private or Sensitive Information (PPSI) is transmitted (including, but not limited to, e-mail, File Transfer Protocol (FTP), instant messaging, e-fax, Voice Over Internet Protocol (VoIP), etc.).
    2. When encryption of data in transit is prescribed by law or regulation.
    3. When connecting to the State internal network(s) over a wireless network.
    4. When remotely accessing the State internal network(s) or devices over a shared (e.g., Internet) or personal (e.g., Bluetooth, infrared) network. This does not apply to remote access over a State managed point to point dedicated connection.

5. When data is being transmitted with a State public facing website and/or web services, they are required to utilize Hypertext Transfer Protocol Secure (HTTPS) in lieu of Hypertext Transfer Protocol (HTTP). State public facing websites must automatically redirect HTTP requests to HTTPS websites. Minimum browser support is listed in Appendix C.

Appropriate encryption methods for data in transit include, but are not limited to, Transport Layer Security (TLS) 1.2 or later, Secure Shell (SSH) 2.0 or later, Wi-Fi Protected Access (WPA) version 2 or later (with Wi-Fi Protected Setup disabled) and encrypted Virtual Private Networks (VPNs). Components should be configured to support the strongest cipher suites possible. Ciphers that are not compliant with this standard must be disabled.

3. **Hash Check**:
   A hash check should be used to ensure that contents of a file have not been modified. Users must generate a hash value (SHA-256 recommended) of a file before it is transmitted which is then compared to a hash value generated upon delivery. The recipient verifies that the hash values match. Performing a hash check verifies that the file was not modified in an unauthorized or undetected manner thus maintaining the security principal of integrity.

   Note: hash value must be communicated between the sender and recipient using an out-of-band method.

4. **Digital signatures**:
   Digital signatures can be used to validate the authenticity of digital messages or documents. A valid digital signature provides the security principals of authentication (recipient has reason to believe that the message or document was created by a known sender), non-repudiation (sender cannot deny having sent the message or document), and integrity (message was not altered in transit).

5. **Data**:
   CBOEs shall only transmit the minimum required data set for a given request/activity. CBOE shall not send data elements that are not necessary in any transmission.

Recommendations for Election Night Reporting (ENR) of Unofficial Results (Options 1 – 4)

Option 1: CD-R/DVD-R

Recommendation: Write (a.k.a. burn) xml file(s) to a CD-R or DVD-R using the CD/DVD writer installed in the EMS server to transfer xml file(s) from the EMS closed network to NYSVoter VPN open network. If the EMS server does not have the capability to write to a CD-R or DVD-R, then an external writer may be attached to the EMS server.

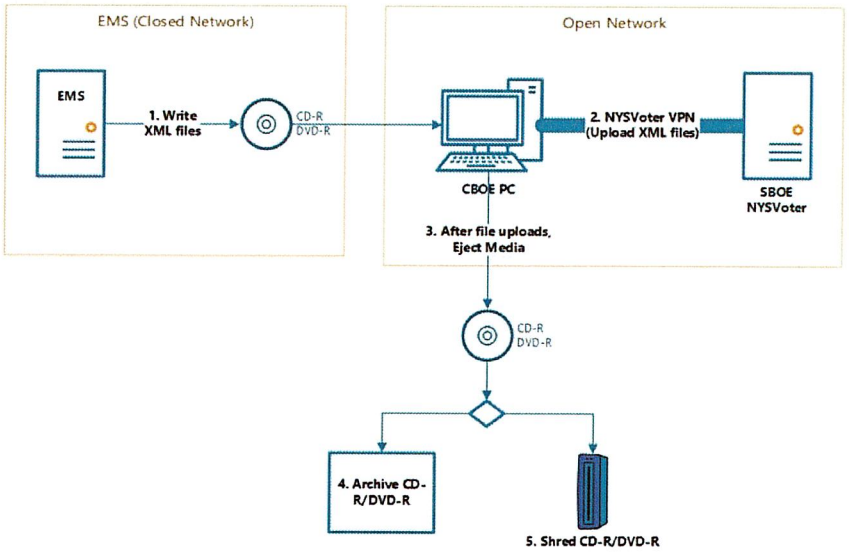
Rationale: The CD-R or DVD-R is write-once technology that uses pristine media that does not contain data, files, applications or executables that would introduce viruses or malware to the closed network devices. After the successful transmission of xml file(s), the CD-R or DVD-R should be either archived or shredded based on the CBOE procedures.

Steps:

1. Write xml file(s) to CD-R/DVD-R (closed network EMS server)
2. Insert CD-R/DVD-R into the open network PC that connects to the NYSVoter VPN and upload (transmit) xml files
3. After file uploads, eject CD-R/DVD-R from the open network PC and perform one of two options
4. Archive CD-R/DVD-R (XML files) or
5. Shred CD-R/DVD-R

For subsequent uploads, use a new CD-R/DVD-R to transfer unofficial results from the EMS closed network.

Figure: 1



Option 2: USB write blocker with dedicated ENR USB flash drive

Recommendation: Use a USB write blocker in conjunction with a dedicated election night reporting (ENR) USB flash drive (a.k.a. thumb drive) to transfer xml files from the EMS closed network to NYSVoter VPN open network.

Rationale: The open network PC will only have 'read' access to the dedicated ENR USB flash drive as the write blocker device will not allow any data, files, applications or executables to be written to the dedicated ENR USB flash drive.

Preconditions:

- Dedicated ENR USB flash drive is sanitized before use on election night
- USB write blocker available for use

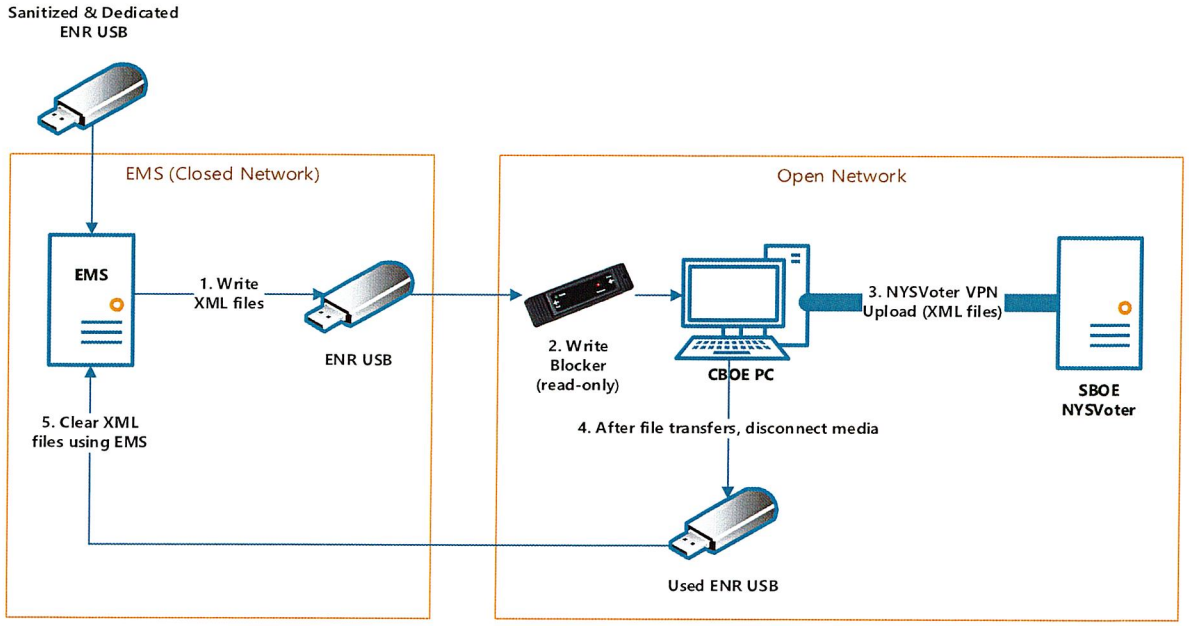
Steps:

1. Write xml file(s) to a dedicated ENR USB flash drive (closed network EMS server)
2. Insert the USB write blocker into the open network PC that connects to the NYSVoter VPN and then insert the dedicated ENR USB flash drive into USB write blocker
3. Upload (transmit) xml files
4. Disconnect dedicated ENR USB flash drive from write blocker and then disconnect the write blocker from the open network PC
5. Insert dedicated ENR USB flash drive into closed network EMS and clear XML files. Dedicated ENR USB flash drive is now ready for next use in the EMS closed network

Note:

1. Human error is always the weakest security link. This recommendation relies on election staff to always use the write blocker whenever the removable media is inserted to a device outside of the closed network.
2. If chain-of-custody of the dedicated ENR USB flash drive cannot be maintained, then the dedicated ENR USB flash drive cannot be used in the EMS closed network environment. If CBOEs want to continue to use the dedicated ENR USB for other activities not related to the closed network, the CBOE must scan, securely reformat and relabel the USB flash drive before use.

Figure: 2



Option 3: Dedicated ENR USB flash drive with physical write protect switch

Recommendation: Use a dedicated ENR USB flash drive with a physical write protect switch and digitally signed secure firmware to transfer xml files from the EMS closed network to NYSVoter VPN open network.

Rationale: The open network PC will only have read access to the dedicated ENR USB flash drive as the physical write protect switch will not allow any data, files, applications or executables to be written to the dedicated ENR USB flash drive. Furthermore, the use of digitally signed secure firmware is used to confirm the author and provide assurance that the firmware code had not been changed since it was signed.

Preconditions: Dedicated ENR USB flash drive:

- With physical write protect switch
- Sanitized before use on election night
- Physical write protect switch was 'On' anytime the dedicated ENR USB flash drive was used outside of the EMS closed network

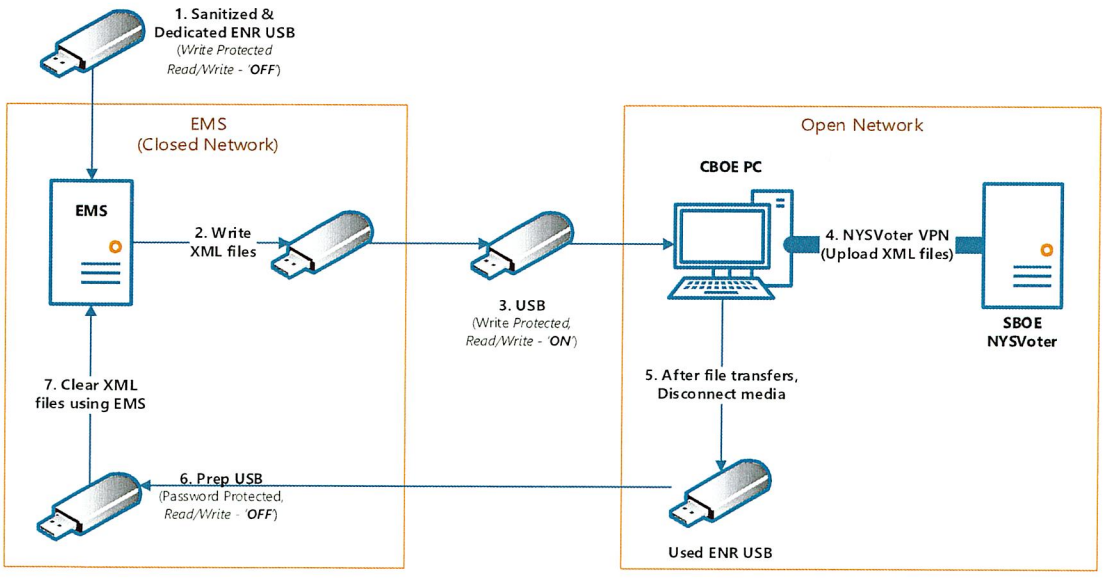
Steps:

1. Select 'Off' (write enabled) position using the physical write protect switch on the dedicated ENR USB flash drive and insert into closed network EMS server
2. Write xml file(s) to a dedicated ENR USB flash drive
3. Eject dedicated ENR USB flash drive from EMS server and select 'On' (write disabled) using the physical write protect switch on the dedicated ENR USB flash drive
4. Insert dedicated ENR USB flash drive into the open network PC that connects to the NYSVoter VPN and upload (transmit) xml files
5. Disconnect dedicated ENR USB flash drive from open network PC that connects to the NYSVoter VPN
6. Select 'Off' (write enabled) using the physical write protect switch on the dedicated ENR USB flash drive
7. Insert dedicated ENR USB flash drive into closed network EMS and clear XML files. Dedicated ENR USB flash drive is now ready for next use in the EMS closed network

Note:

1. Human error is always the weakest security link. This recommendation relies on election staff to physically manipulate a write protect switch located on the USB.
2. If chain-of-custody of the dedicated ENR USB flash drive cannot be maintained, then the dedicated ENR USB flash drive cannot be used in the EMS closed network environment. If CBOEs want to continue to use the dedicated ENR USB for other activities not related to the closed network, the CBOE shall scan and securely reformat and relabel the USB flash drive before use.

Figure: 3



Option 4: Media eraser with dedicated USB flash drive

Recommendation: Use a media eraser in conjunction with a dedicated election night reporting (ENR) USB flash drive (a.k.a. thumb drive) to transfer xml files from the EMS closed network to NYSVoter VPN open network.

Rationale: The media eraser will be used on the dedicated election night reporting (ENR) USB flash drive (a.k.a. thumb drive) that was used to transfer results from the closed network to the open network. This will fully erase the contents of the ENR USB flash drive before being used on the CBOE closed network.

Preconditions:

- Dedicated ENR USB flash drive sanitized before use on election night.
- Media eraser available at the CBOE.

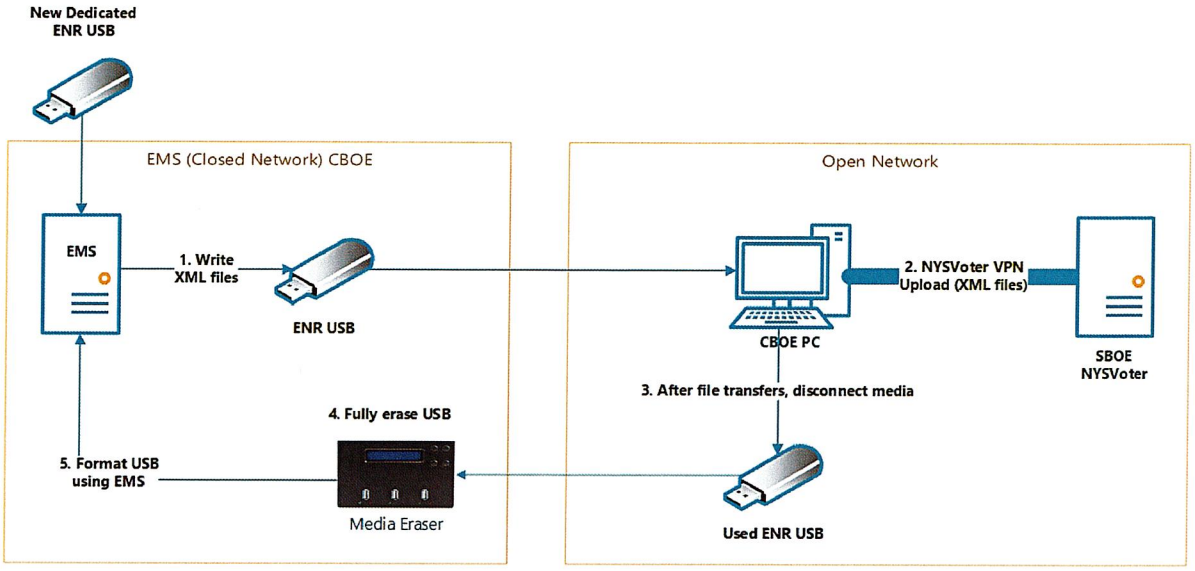
Steps:

1. Write xml file(s) to a dedicated ENR USB flash drive (closed network EMS server)
2. Insert dedicated ENR USB flash drive into open network PC and upload (transmit) xml files
3. Disconnect dedicated ENR USB flash drive from the open network PC
4. Insert dedicated ENR USB flash drive into the media eraser to erase all contents
5. Insert dedicated USB into the closed network EMS to perform a high-level reformat. Dedicated USB media ready for use.

Note:

1. Human error is always the weakest security link. This recommendation relies on election staff to fully erase and reformat the USB flash drive before next use.
2. If chain-of-custody of the dedicated ENR USB flash drive cannot be maintained, then the dedicated ENR USB flash drive cannot be used in the EMS closed network environment. If CBOEs want to continue to use the dedicated ENR USB for other activities not related to the closed network, the CBOE shall scan and securely reformat and relabel the USB flash drive before use.

Figure: 4



5a. Transfer of Unofficial Poll Site Results after the Closing of the Polls (Write Blocker)

Recommendation: Use a write blocker in conjunction with the removable media from each PBOS (USB – ES&S, CF Card – Dominion) to transfer unofficial election results files from an Election Night Results Transfer Site to the CBOE Uncertified Reporting tool via an open network configured by the CBOE.

Rationale: The CBOE Transfer Device will only have read access to the dedicated PBOS removable media as the write blocker device will not allow any data, files, applications or executables to be written to the PBOS removable media.

Preconditions: Write blocker based on removable media being used.

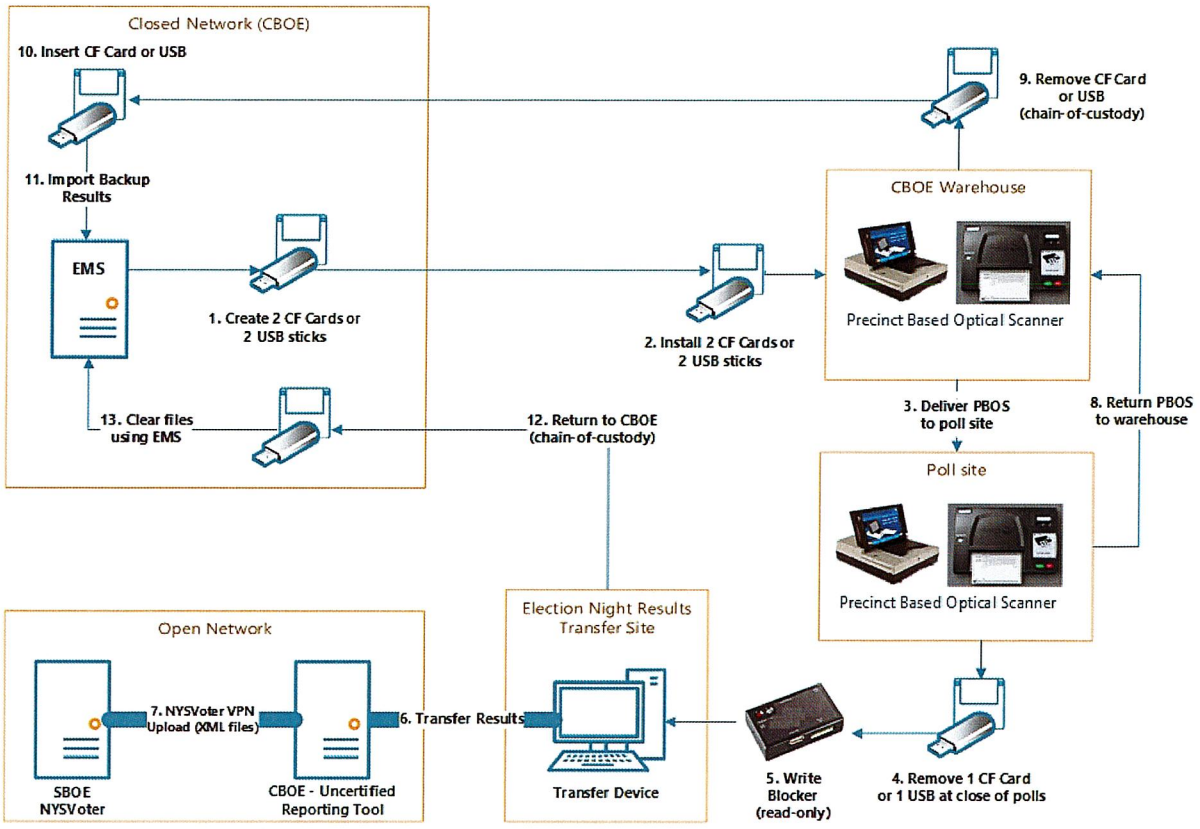
Steps from diagram:

5. Insert write blocker into CBOE Transfer Device that connects via an open network to the CBOE Uncertified Reporting Tool and insert PBOS removable media (containing unofficial election results files) into write blocker device (each PBOS)
6. Transmit (transfer) unofficial election results files
12. Disconnect PBOS removable media from the write blocker, disconnect write blocker from the CBOE Transfer Device and transport removable media back to the CBOE
13. After an election has been certified and archiving activities are completed for the 24-month period requirement (NYS Election Law Section 3-222), insert PBOS removable media used in the election into the closed network EMS to perform a high-level reformat. PBOS removable media ready for use.

Note:

1. Human error is always the weakest security link. This recommendation relies on election staff to always use the write blocker whenever the removable media is inserted to a device outside of the closed network.
2. If chain-of-custody of removable media cannot be maintained, then the removable media cannot be used in the EMS closed network or PBOS in future elections. If CBOEs wants to use the removable media for other activities not related to the closed network, the CBOE shall scan and securely reformat and rename the removable media before use.

Figure: 5a



5b. Transfer of Unofficial Poll Site Results after the Closing of the Polls (Media Eraser)

Recommendation: Use a media eraser on the removable media from each PBOS (USB – ES&S, CF Card – Dominion) that were used to transfer unofficial election results files from an Election Night Results Transfer Site to the CBOE Uncertified Reporting tool via an open network configured by the CBOE.

Rationale: The media eraser will be used on each removable media PBOS (USB – ES&S, CF Card – Dominion) that was used in conjunction CBOE Election Night Results Transfer Site Device. The media eraser will erase the contents before being used on the CBOE closed network.

Preconditions:

- Media eraser available at the CBOE
- Chain-of-custody is maintained throughout the entire process

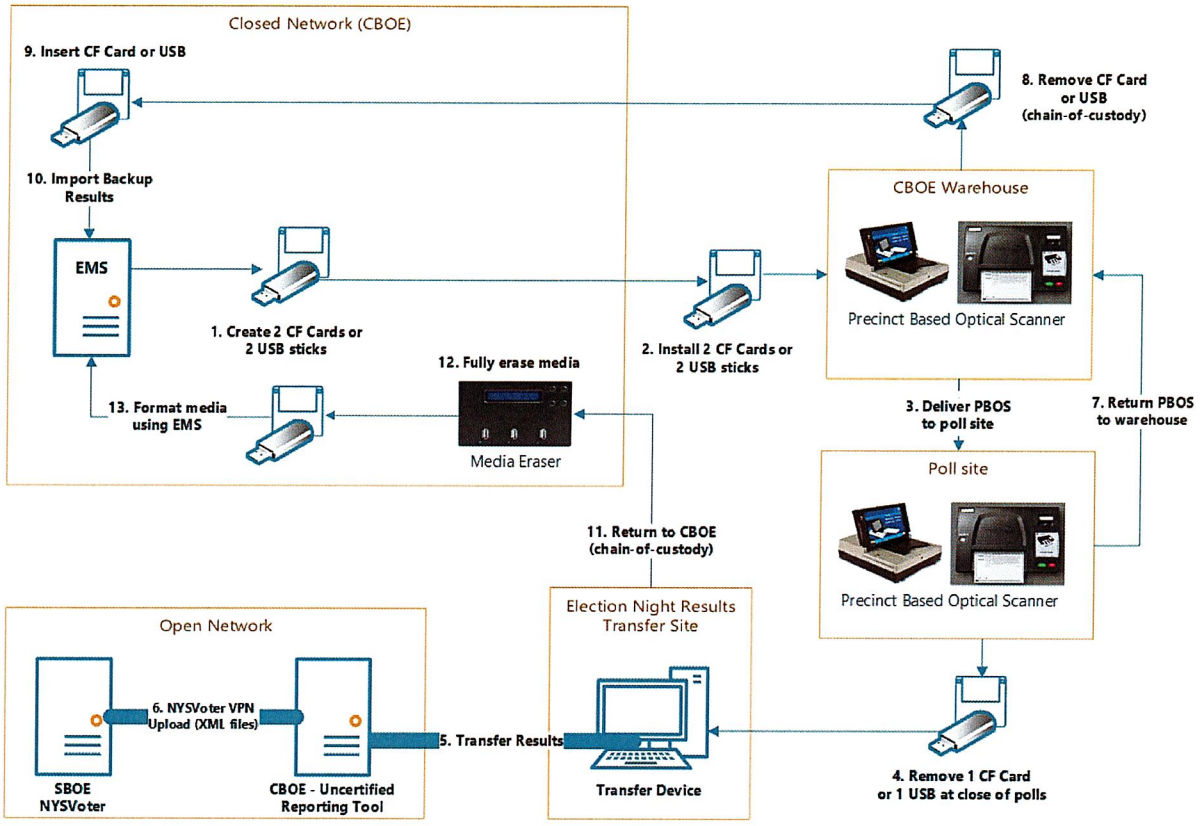
Steps from diagram:

5. Transmit (transfer) unofficial election results files
11. Return PBOS removable media to CBOE using chain-of-custody procedures
12. After an election has been certified and archiving activities are completed for the 24-month period requirement (NYS Election Law Section 3-222), use the media eraser to erase all contents on each PBOS removable media used for Election Night Results reporting.
13. Insert all PBOS removable media used in the election into the closed network EMS to perform a high-level reformat. PBOS removable media ready for use.

Note:

1. Human error is always the weakest security link. This recommendation relies on election staff to always use the media eraser whenever the removable media is inserted to a device outside of the closed network.
2. If chain-of-custody of removable media cannot be maintained, then the removable media cannot be used in the EMS closed network or PBOS in future elections. If CBOEs wants to use the removable media for other activities not related to the closed network, the CBOE shall scan and securely reformat and rename the removable media before use.

Figure: 5b



6a. Transfer of Ballot PDFs to Print Vendor (Write Blocker)

Recommendation: Use a USB write blocker in conjunction with a dedicated Ballot PDF Transfer USB flash drive (a.k.a. thumb drive) to transfer ballot PDFs from the EMS closed network to a PC connected on the CBOE open network.

Rationale: The open network PC will only have read access to the dedicated Ballot PDF Transfer USB flash drive as the write blocker device will not allow any data, files, applications or executables to be written to the dedicated ENR USB flash drive.

Preconditions:

1. Dedicated Ballot PDF Transfer USB flash drive sanitized before use
2. USB write blocker was connected anytime the PDF Transfer USB flash drive was used outside of the EMS closed network
3. Each CBOE shall have a process in place to visually verify the ballot PDFs to ensure the integrity of the data was maintained by the vendor when printing the ballots. Once the ballot PDFs are visually verified as correct, the CBOE shall provide sign-off on the ballots.

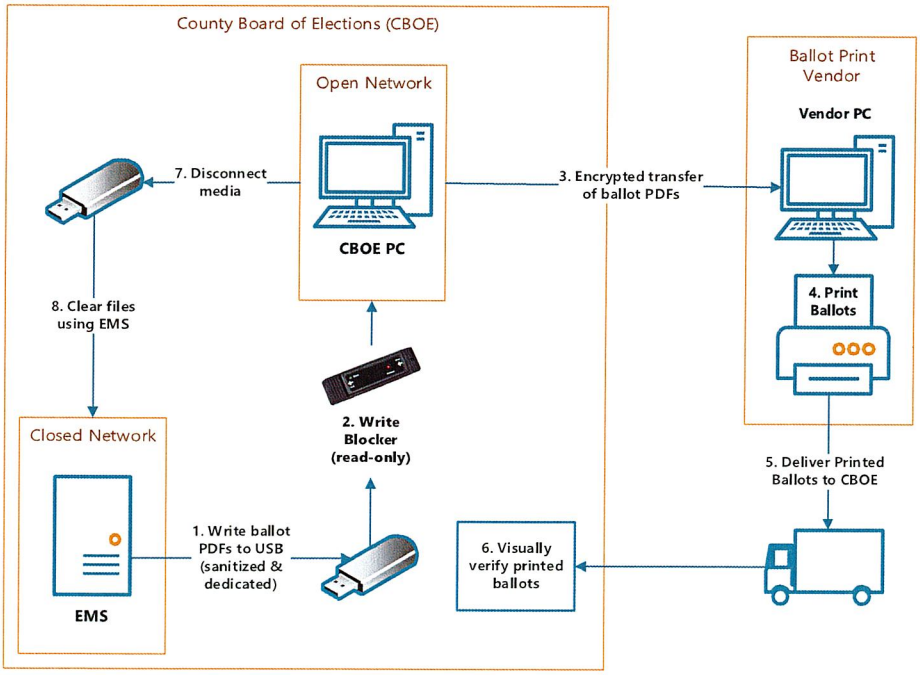
Steps from diagram:

1. Write ballot PDFs to a dedicated Ballot PDF Transfer USB flash drive (closed network EMS server)
2. Transfer ballot PDFs
5. Visually verify printed ballots against submitted PDFs following CBOE defined process and procedures
6. Disconnect dedicated Ballot PDF Transfer USB flash drive from the open network PC
7. Insert dedicated Ballot PDF Transfer USB flash drive into the media eraser to delete all contents
8. Insert dedicated USB into the closed network EMS to perform a high-level reformat. Dedicated USB media ready for use

Note:

1. Human error is always the weakest security link. This recommendation relies on election staff to fully erase and reformat the USB flash drive before next use.
2. If chain-of-custody of the dedicated Ballot PDF Transfer USB flash drive cannot be maintained, then the dedicated Ballot PDF Transfer USB flash drive cannot be used in the EMS closed network environment. If CBOEs want to continue to use the dedicated Ballot PDF Transfer USB for other activities not related to the closed network, the CBOE shall scan and securely reformat and relabel the USB flash drive before use.

Figure: 6a



6b. Transfer of Ballot PDFs to Print Vendor (Media Eraser)

Recommendation: Use a media eraser in conjunction with a dedicated Ballot PDF Transfer USB flash drive (a.k.a. thumb drive) to transfer ballot PDFs from the EMS closed network to a PC connected on the CBOE open network.

Rationale: The media eraser will be used on the dedicated Ballot PDF Transfer USB flash drive (a.k.a. thumb drive) that was used to transfer ballot PDFs from the closed network to the open network. The media eraser will fully erase the contents before being used on the CBOE closed network.

Preconditions:

1. Dedicated Ballot PDF Transfer USB flash drive flash drive sanitized before use
2. Media eraser available at the CBOE
3. Each CBOE shall have a process in place to visually verify the ballot PDFs to ensure the integrity of the data was maintained by the vendor when printing the ballots. Once the ballot PDFs are visually verified as correct, the CBOE shall provide sign-off on the ballots.

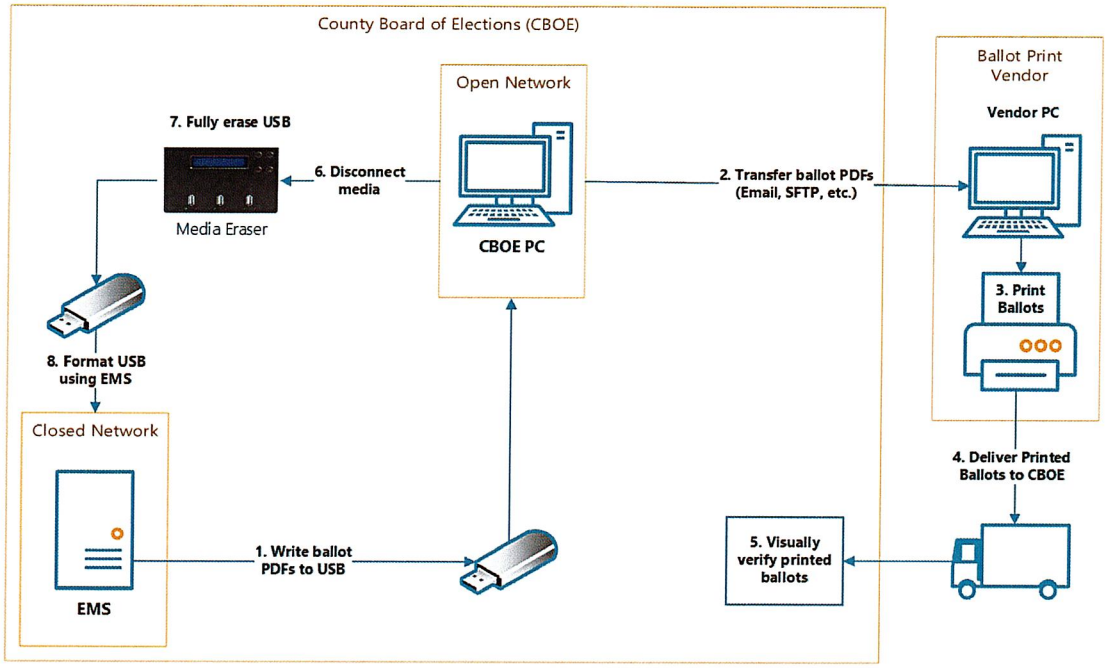
Steps from diagram:

1. Write ballot PDFs to a dedicated Ballot PDF Transfer USB flash drive (closed network EMS server)
2. Insert the USB into open network PC that transfers ballot PDFs to the print vendor and transfer ballot PDFs
5. Visually verify printed ballots against submitted PDFs following CBOE defined process and procedures
6. Disconnect dedicated Ballot PDF Transfer USB flash drive from the open network PC
7. Insert dedicated ENR USB flash drive into the media eraser to erase all contents.
8. Insert dedicated USB into the closed network EMS to perform a high-level reformat. Dedicated USB media ready for use.

Note:

1. Human error is always the weakest security link. This recommendation relies on election staff to always use the media eraser whenever the removable media is inserted to a device outside of the closed network.
2. If chain-of-custody of the dedicated Ballot PDF Transfer USB flash drive cannot be maintained, then the dedicated Ballot PDF Transfer USB flash drive cannot be used in the EMS closed network environment. If CBOEs want to continue to use the dedicated Ballot PDF Transfer USB for other activities not related to the closed network, the CBOE shall scan and securely reformat and relabel the USB flash drive before use.

Figure: 6b



7a. Transfer of Bridge Data from Vendor to CBOE (CD-R/DVD-R)

Recommendation: Scan downloaded bridge data file(s) with anti-virus and anti-malware software. If no threats are found, write (a.k.a. burn) bridge data files to a write-once CD-R or DVD-R using the CD/DVD writer installed on an open network PC. If the open network PC does not have the capability to write to a CD-R or DVD-R, then an external writer may be attached to the PC.

Rationale: The CD-R or DVD-R is write-once technology that uses pristine media that does not contain data, files, applications and executables that would introduce viruses or malware to the closed network. After the successful import of bridge data files, the CD-R or DVD-R is to be shredded.

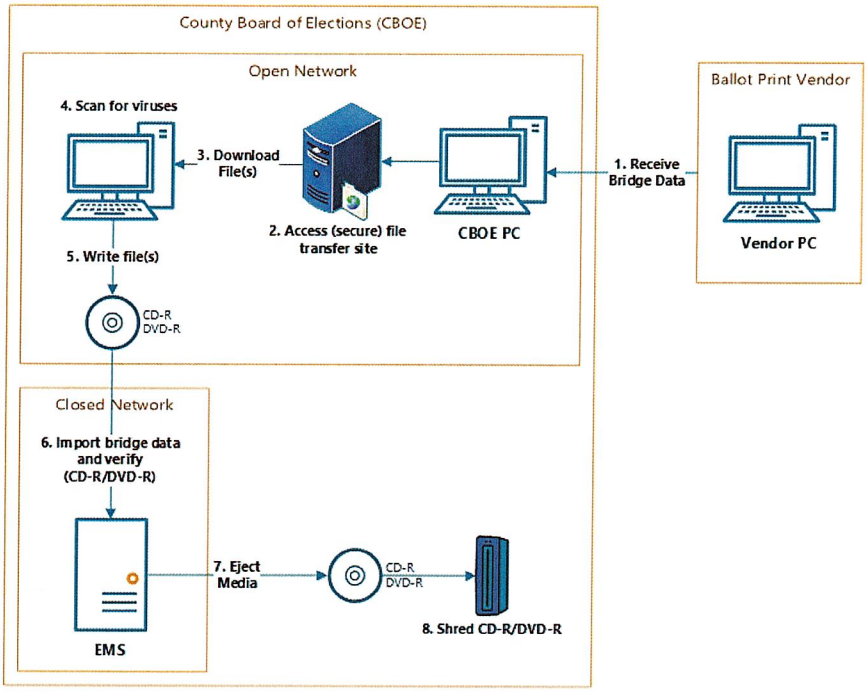
Precondition: Each CBOE shall have a process in place to visually verify the data points to ensure the integrity of the data received from the vendor. Once the data is verified as correct, the CBOE shall provide sign-off on the data.

Steps:

1. Receive bridge data files
2. Access (secure) file transfer site
3. Download bridge data files
4. Scan files for viruses and malware
5. Write files to CD-R/DVD-R (if no threats were found)

6. Insert CD-R/DVD-R into the EMS closed network, import bridge data files into EMS and manually verify data accuracy
7. Eject CD-R/DVD-R from the EMS closed network
8. Shred CD-R/DVD-R. Use new CD-R/DVD-R for next use in the EMS closed network

Figure: 7a



7b. Transfer of Bridge Data from Vendor to CBOE (Media Eraser)

Recommendation: Use a media eraser in conjunction with scanning downloaded bridge data file(s) with anti-virus and anti-malware software. If no threats are found, write bridge data files to a dedicate bridge data USB flash drive.

Rationale: The media eraser will be used on the dedicated bridge data USB flash drive (a.k.a. thumb drive) that was used to transfer bridge data from CBOE open network to the CBOE closed network. The media eraser will fully erase the contents before each download.

Precondition:

- Each CBOE shall have a process in place to visually verify the data points to ensure the integrity of the data received from the vendor. Once the data is verified as correct, the CBOE shall provide sign-off on the data.
- Dedicated bridge data USB flash drive sanitized before use.
- Media eraser available at the CBOE

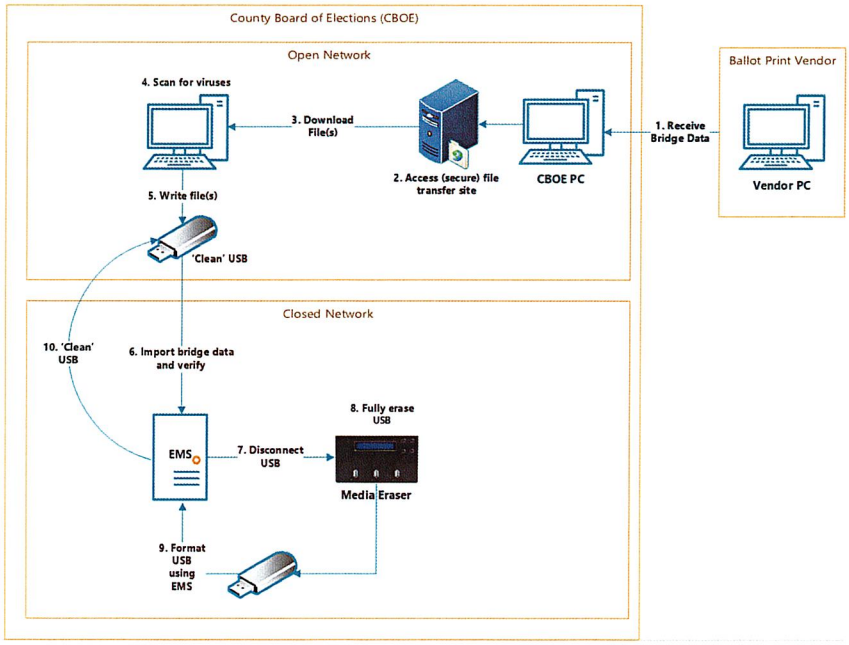
Steps:

1. Receive bridge data files
2. Access (secure) file transfer site
3. Download bridge data files
4. Scan files for viruses and malware
5. Write files to dedicated bridge data USB flash drive (if no threats were found)
6. Insert dedicated bridge data USB flash drive into the EMS closed network, import bridge data files into EMS and manually verify data accuracy
7. Disconnect dedicated bridge data USB flash drive from the EMS closed network
8. Insert dedicated bridge data USB flash drive into the media eraser to erase all contents
9. Insert dedicated USB into the closed network EMS to perform a high-level reformat
10. Dedicated bridge data USB flash drive ready for use 'Clean USB'

Note:

1. Human error is always the weakest security link. This recommendation relies on election staff to always use the media eraser whenever the removable media is inserted to a device outside of the closed network.
2. If chain-of-custody of the dedicate bridge data USB flash drive cannot be maintained, then the dedicate bridge data USB flash drive cannot be used in the EMS closed network environment. If CBOEs want to continue to use the dedicate bridge data USB flash drive for other activities not related to the closed network, the CBOE shall scan and securely reformat and relabel the USB flash drive before use.

Figure: 7b



8a. Data Imports into EMS

Recommendation: Scan data import file(s) with anti-virus and anti-malware software. If no threats are found, write (a.k.a. burn) data import files to a write-once CD-R or DVD-R using the CD/DVD writer installed on an open network PC. If the open network PC does not have the capability to write to a CD-R or DVD-R, then an external writer may be attached to the PC.

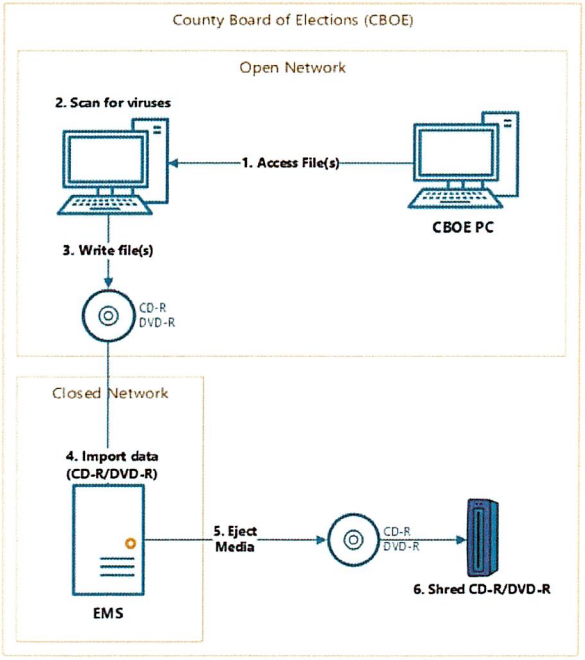
Rationale: The CD-R or DVD-R is write-once technology that uses pristine media that does not contain data, files, applications and executables that would introduce viruses or malware to the closed network. After the successful import of data files, the CD-R or DVD-R is to be shredded.

Precondition: Each CBOE shall have a process in place to visually verify the data points to ensure the integrity of the data. Once the data is visually verified as correct, the CBOE shall provide sign-off on the data.

Steps:

1. Access data import files on CBOE PC
2. Scan files for viruses and malware
3. Write files to CD-R/DVD-R (if no threats were found)
4. Insert CD-R/DVD-R into the EMS closed network and import bridge data files into EMS and visually verify data accuracy
5. Eject CD-R/DVD-R from the EMS closed network
6. Shred CD-R/DVD-R. Use new CD-R/DVD-R for next use in the EMS closed network

Figure: 8a



8b. Data Imports into EMS (Media Eraser)

Recommendation: Use a media eraser in conjunction with scanning data import file(s) with anti-virus and anti-malware software. If no threats are found, write data import files to a dedicate data import USB flash drive.

Rationale: The media eraser will be used on the dedicated data import USB flash drive (a.k.a. thumb drive) that was used to transfer data import files from CBOE open network to the CBOE closed network. The media eraser will fully erase the contents before each copy/transfer.

Precondition:

- Each CBOE shall have a process in place to visually verify the data points to ensure the integrity of the data. Once the data is verified as correct, the CBOE shall provide sign-off on the data.
- Dedicated data import USB flash drive sanitized before use
- Media eraser appliance available at the CBOE

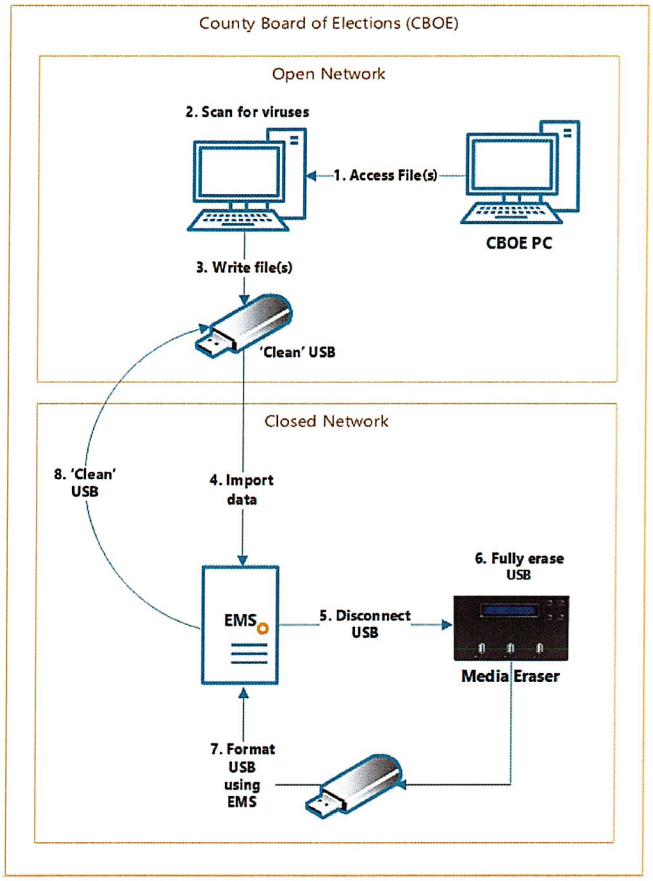
Steps:

1. Access data import files on CBOE PC
2. Scan files for viruses and malware
3. Write files to dedicate data import USB flash drive (if no threats were found)
4. Insert dedicated data import USB flash drive into the EMS closed network, import files into EMS and manually verify data accuracy
5. Disconnect dedicated data import USB flash drive from the EMS closed network
6. Insert dedicated data import USB flash drive into the media eraser to erase all contents
7. Insert dedicated USB into the closed network EMS to perform a high-level reformat
8. Dedicated data import USB flash drive ready for use 'Clean USB'

Note:

1. Human error is always the weakest security link. This recommendation relies on election staff to always use the media eraser whenever the removable media is inserted to a device outside of the closed network.
2. If chain-of-custody of the dedicated data import USB flash drive cannot be maintained, then the dedicated data import USB flash drive cannot be used in the EMS closed network environment. If CBOEs want to continue to use the dedicated data import USB flash drive for other activities not related to the closed network, the CBOE shall scan and securely reformat and relabel the USB flash drive before use.

Figure: 8b



9. Transfer of Poll Book Data to Print Vendor

Recommendation (Outsource Printing): Use Microsoft Word 2013 or later version 'Encrypt with Password' feature to encrypt poll book data file(s) to be sent to the print vendor using the default values (Advanced Encryption Standard (AES), 128-bit key length, SHA1, and cipher block chaining (CBC)). Passwords shall be created using NYS ITS IT Policy: Identity Assurance (NYS-P10-006), IT Standard: Identity Assurance (NYS-S13-004) and IT Standard: Authentication Tokens (NYS-S14-006). Passwords shall be communicated from the CBOE to the Poll Book Print Vendor using out-of-band methods such as by phone (voice) or text message to a confirmed number. Encrypted poll book data files shall be transferred from the CBOE to Poll Book Print Vendor using one of the secure file transfer options listed in the 'Best Practices for Transmission of Files and Data' section.

Rationale: Using Microsoft's built in encryption features to encrypt poll book data files will provide a layer of protection to ensure the confidentiality of the data is not compromised. Poll book data files include but are not limited to the following fields: full name, address, birth date, date of registration, and signature.

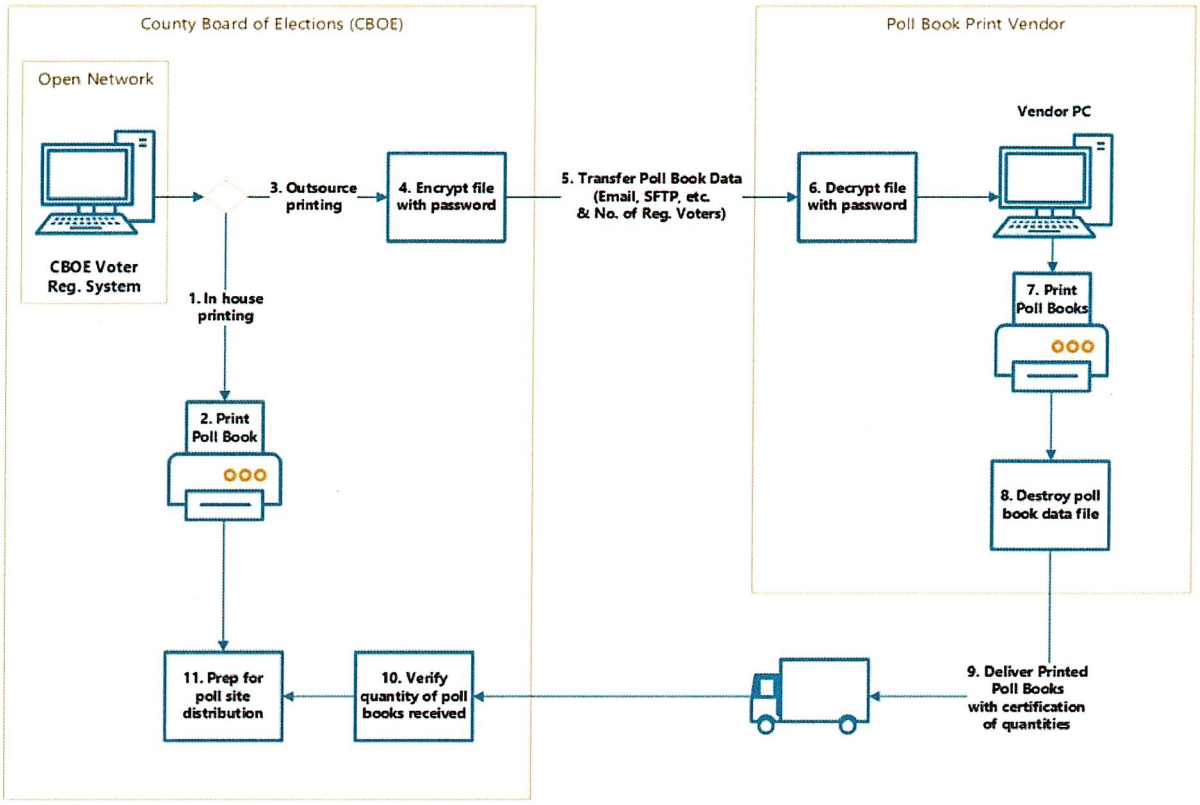
Preconditions:

1. Poll book (voter registration) data confirmed for printing. The CBOE shall only transmit the minimum required voter registration fields needed to print the poll book. The CBOE shall not send data fields that are not required to print the poll book.
2. Each CBOE shall have a process and procedure in place to manually verify quantity of poll books received against the print vendor certification and number of registered voters. Once the data is confirmed as correct, the CBOE shall provide sign-off on the data.
3. Microsoft Word 2013 or later version.

Steps from diagram:

3. CBOE decision to outsource printing of poll books
4. CBOE uses Microsoft Word 2013 or later 'Encrypt with Password' feature to encrypt poll book data files with a password. CBOE will send password to poll book print vendor using predetermined out-of-band method.
5. CBOE transfers poll book data along with the number of registered voters contained in the file.
6. Poll book print vendor decrypts poll book data file(s) with password obtained out-of-band from CBOE
7. Poll book print vendor processes data file(s) and prints poll books.
8. Poll book print vendor will destroy poll book data file received from the CBOE by deleting all instances of file from their system
9. Poll book print vendor will deliver printed poll books to the CBOE with a certification of quantities produced. The poll book print vendor will also certify to the CBOE the number of registered voters processed and included in the poll books.
10. CBOE will manually verify quantity of poll books received against the print vendor certification and number of registered voters.
11. CBOE prepare the poll books for distribution to poll sites.

Figure: 9



10. Updating Static Website Data

Recommendation (Third Party Vendor): Use a hash value application to generate a SHA256 hash value for associated website data file(s). Hash value(s) shall be entered into a Microsoft Word 2013 or later version document and encrypted using the 'Encrypt with Password' feature. The password encrypted document containing the hash values can be emailed to the Third-Party Vendor. Passwords shall be created using NYS ITS IT Policy: Identity Assurance (NYS-P10-006), IT Standard: Identity Assurance (NYS-S13-004) and IT Standard: Authentication Tokens (NYS-S14-006). Passwords shall be communicated from the CBOE to the Third-Party Vendor using out-of-band methods such as by phone (voice) or text message to a confirmed number. Website data files shall be transferred from the CBOE to Third Party Vendor using one of the secure file transfer options listed in the 'Best Practices for Transmission of Files and Data' section.

Rationale: Using a hash value application to generate hash values for the files that will be transmitted to the third-party vendor will ensure the integrity of the data is not compromised.

Preconditions:

1. Website files confirmed for posting
2. Microsoft Word 2013 or later version

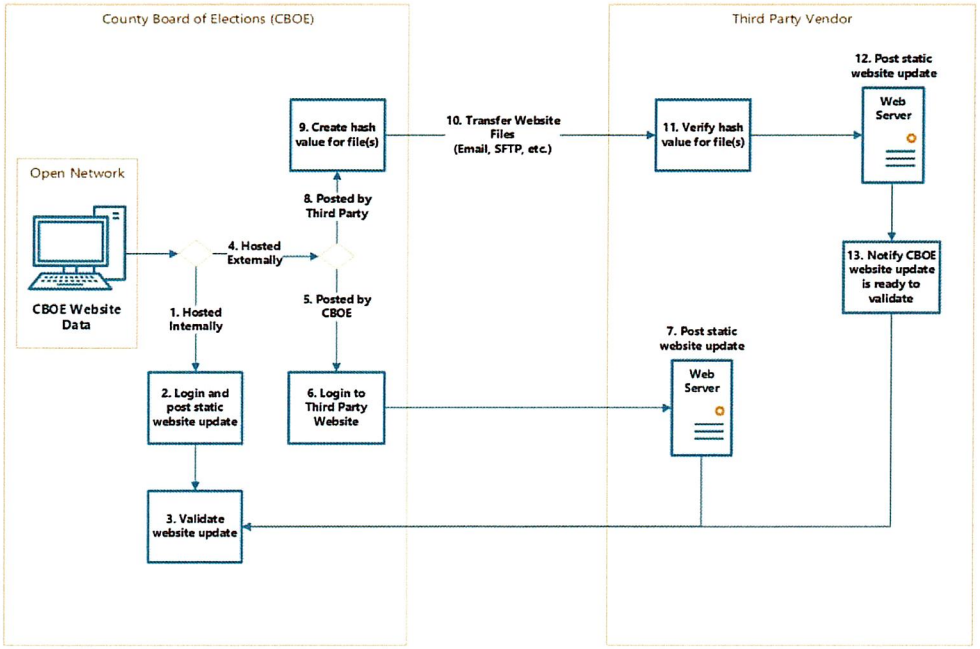
Note: Each CBOE shall have a process in place to visually verify website content updates (for both internally and externally hosted sites) to ensure that integrity was maintained. Once the website updates are verified as correct, the CBOE shall provide sign-off.

Steps from diagram:

8. CBOE decision to have third party post website updates
9. CBOE uses a hash value application to generate a SHA256 hash value on website update files. CBOE will send hash value(s) to third party vendor (website) using predetermined out-of-band method
10. CBOE transfers website files using secure method
11. Third party vendor verifies hash values on transmitted files with password obtained out-of-band from CBOE
12. Third party vendor updates CBOE website
13. Third party vendor notifies CBOE that website has been updated and is ready to validate
3. CBOE validates website content for accuracy

Hash Value Generator: CBOE should use the hash calculator application they use when performing hash checks on voting systems. SlavaSoft HashCalc 2.02 is the latest version available for download at: http://www.slavasoft.com/?source=HashCalc.exe

Figure: 10



11. Election System Upgrades

Step 3 – Receive Trusted Build Media (Decrypt, Verify Hashes)

Actor: SBOE

Usage: The SBOE Election Operations Unit must use a PC to:

- Decrypt the trusted build media using the password provided by the VSTL
- Verify the hash values of the trusted build files provided by the VSTL
- Save trusted build file(s) to a shared drive located on the SBOE local area network (LAN)
- Archive trusted build media

Recommendation: The SBOE Election Operations Unit shall use a PC that is:

- Designated only for trusted build activities
- Hardened per SBOE IT policy
- Hardened per NIST best practices
- Up to date on all patches
- Up to date on anti-virus/anti-malware definitions
- Shared drive is only accessible by Election Operations Unit

Rationale: System hardening (configuration steps) must be applied to a system to ensure that the system is resilient to attack or compromise.

Step 5 – Create Final Build (Media)

Actor: SBOE

Recommendation: The SBOE Election Operations Unit will continue using write-once media (CD-R or DVD-R) to write (a.k.a. burn) final build file(s) to a CD-R or DVD-R using the CD/DVD writer installed in the designated 'trusted build' PC. If the PC does not have the capability to write to a CD-R or DVD-R, then an external writer may be attached to the PC.

Rationale: The CD-R or DVD-R is write-once technology that uses pristine media that does not contain data, files, applications and executables that would introduce viruses or malware to the closed network. After the successful import of bridge data files, the CD-R or DVD-R is to be archived. Insecure methods of transfer increase the risk of compromising the integrity.

Step 7 – Validate hash values (media & files)

Actor: CBOE

Usage: The CBOE must use a PC to:

- Verify the hash value of the final build media provided by SBOE Election Operations Unit
- Verify the hash values of the final build files provided by the VSTL

Recommendation: The CBOE shall use a PC that is:

- Designated only for upgrade and hash check activities

- Standalone PC/Laptop (non-networked with CD-RW/DVD-RW drive)
- Hardened per county IT policy
- Hardened per NIST best practices
- Up to date on all patches
- Up to date on anti-virus/anti-malware definitions

Rationale: System hardening (configuration **s**teps) must be applied to a system to ensure that the system is resilient to attack or compromise. A compromised PC could subvert the hash check procedure; therefore, the PC should be standalone.

Step 11 – Load Final Build (Upgrade removed from CD/DVD)
Step 12 – Transfer Image(s)/File(s)
Actor: CBOE
Usage: The CBOE must use a PC to:

- Transfer images
    - Use SelfImage application to write image from transfer PC/laptop to USB thumb drive DS200 (ES&S proprietary media)
    - Use SelfImage application to write image from transfer PC/laptop to CF Card (DS850 and AutoMARK)
    - Use WinImage application to write image from transfer PC/laptop to CF Card (Dominion BMD upgrade)

PC Recommendation: The CBOE shall use a PC that is:

- Designated only for upgrade and hash check activities
- Standalone PC/Laptop (non-networked with CD-RW/DVD-RW drive)
- Hardened per county IT policy
- Hardened per NIST best practices
- Up to date on all patches
- Up to date on anti-virus/anti-malware definitions

PC Rationale: System hardening (configuration **s**teps) must be applied to a system to ensure that the system is resilient to attack or compromise. A compromised PC could be a potential point where malicious code can be introduced, therefore the PC should be standalone.

Removable Media Recommendation: CBOE shall use removable media that is designated for upgrades or software validations (hash checks) only.

Removable Media Rationale: Removable media used for election day activities cannot be used for system upgrades or software validations if media is inserted into another device that is not considered part of the closed network, unless a write blocker is used. Chain of custody must be maintained on all removable media.

Step 14 – Perform Hash Check (Software Validation)
Actor: CBOE
Usage: The CBOE must use a PC to perform hash checks following associated procedure.

PC Recommendation: The CBOE shall use a PC that is:

- Designated only for upgrade and hash check activities
- Standalone PC/Laptop (non-networked with CD-RW/DVD-RW drive)
- Hardened per county IT policy
- Hardened per NIST best practices
- Up to date on all patches
- Up to date on anti-virus/anti-malware definitions

PC Rationale: System hardening (configuration steps) must be applied to a system to ensure that the system is resilient to attack or compromise. A compromised PC could subvert the hash check procedure, therefore the PC should be standalone.

Removable Media Recommendation:

CBOE shall use removable media that is designated for upgrades or software validations (hash checks) only.

Removable Media Rationale: Removable media used for election day activities cannot be used for system upgrades or software validations if media is inserted into another device that is not considered part of the closed network, unless a write blocker is used. Chain of custody shall be maintained on all removable media.

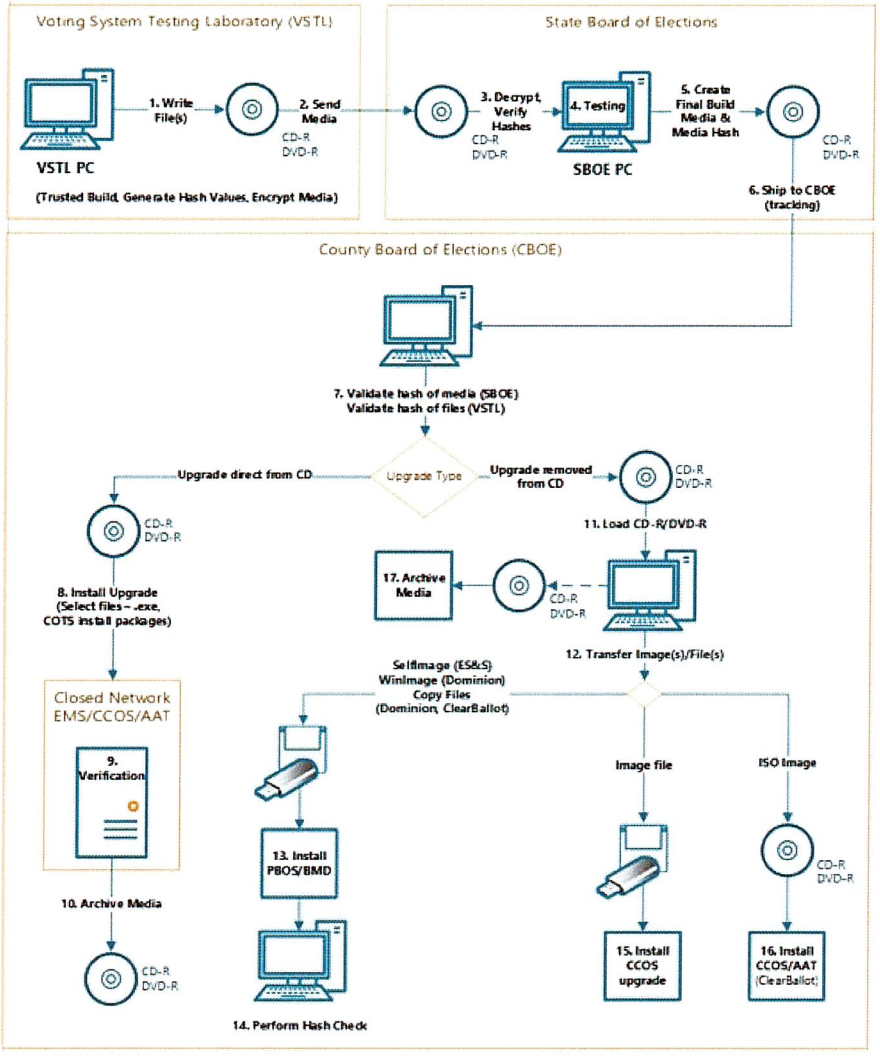
Step 15 – Install CCOS upgrade
Actor: CBOE
Removable Media Recommendation: CBOE shall use removable media that is designated for upgrades or software validations (hash checks) only.

Removable Media Rationale: Removable media used for election day activities cannot be used for system upgrades or software validations if media is inserted into another device that is not considered part of the closed network, unless a write blocker is used. Chain of custody shall be maintained on all removable media.

Step 16 – Install CCOS/AAT upgrade
Actor: CBOE
Removable Media Recommendation: The CBOE writes ISO image to a write-once CD-R or DVD-R media is using the CD/DVD writer installed on the transfer image PC. If the PC does not have the capability to write to a CD-R or DVD-R, then an external writer may be attached to the PC.

Removable Media Rationale: The CD-R or DVD-R is write-once technology that uses pristine media that does not contain data, files, applications and executables that would introduce viruses or malware to the system. After the successful upgrade, the CD-R or DVD-R is to be shredded.

Figure: 11



ONONDAGA COUNTY BOARD OF ELECTIONS

AGREEMENT OF VOTE BY MAIL BALLOT DISTRIBUTION

COMMISSIONERS DUSTIN M. CZARNY and KEVIN P. RYAN

Thursday, July 31, 2025

It is the policy of the Onondaga County Board of Elections that:

- All Vote by Mail ballots are mailed if time is allowed.
- Any person or agent designated on a Vote by Mail application to pick up Vote by Mail ballots for another individual will be granted five (5) Vote by Mail ballots per day. If a person or agent wishes to drop off more than five (5) such applications at a time, there will be a one (1) business day hold on the issuing of the ballots to allow for the BOE to process the applications as well as notify the recipient by mail and phone that a ballot is being issued in their name.
- Vote by Mail applications/ballots will not be given out together more than one (1) week before a Primary or General Election.
- Ballots will be delivered to the post office by commissioners, deputy commissioners or designees of the commissioners.
- Ballots Requested on Election Day can only be issued by court order.

Dustin M. Czarny
Commissioner (D)
Onondaga County Board of Elections

Kevin P. Ryan
Commissioner (R)
Onondaga County Board of Elections

Social Media Calendar August 2025

Mondays

9am – Early Voting Page

Noon – Vote by Mail

3pm – Polling Place Page

Tuesdays

9am – Polling Place Page

noon – Special

3pm – Voter Reg Page

Wednesday

9am – Stats page

Noon – Polling Place Page

3pm – Vote by Mail

Thursday

9am – Election Inspector page

Noon – Early Voting Page

3pm – Polling Place Page

Friday

9am – Voter Reg Page

Noon – Maps Page

3pm – Special

Saturday

9am – Results Page

Noon – Polling Place Page

3pm – Early Voting Page

Sunday

9am – Election Inspector page

Noon – Vote by Mail

3pm – Candidate information Page

Specials

All month Inspector recruitment

Village options for conducting an Election

Revised: July 31, 2025

1. Onondaga County Board of Elections conducts Village Election in November, Village will not be charged for anything.

2. Onondaga County Board of Elections conducts Village Election in March/June, Village will be charged for all costs.

3. Village conducts their own election with their own materials and equipment.

Option #1 - Onondaga County Board of Elections conducts Village Election in November, Village will not be charged for anything.

The Board of Elections will be responsible for all election processes including but not limited to:

- Accepting all petitions, certifications of nominations, acceptances, declinations, authorizations, general and specific objections.
- Preparing candidates list, media releases, candidates notices, etc.
- Processing all absentee applications, absentee ballots, and absentee ballot cures.
- Hiring all applicable staff (inspectors, poll site managers and machine technicians).
- Canvassing all ballots including affidavits.
- Certifying the election and notifying winners.
- Conducting a manual hand count if applicable.

Option #2 - Onondaga County Board of Elections conducts Village Election in March/June.

BOE will conduct all election processes including all filings for ballot access and the Village will be responsible for the following costs:

- Ballot Programming and Machine Pre-Lat =$75.00 per hour (est. 3 hours)
- Ballot Printing (Emergency Ballots) =$.25 per ballot
- Blank Ballot on Demand Paper = $.25 per ballot
- Trucking Cost = *See contracted pricing sheet
- Data Charge (for electronic poll books) = $15.00 per pollpad
- Inspector Pay (BOE will appoint all Inspectors, Village will be responsible for payments) *These are the 2023 rates based on Minimum Wage*
  Minimum of 2 regular inspectors and 2 poll site managers required.
  - Regular Inspector = $15.50 per hour (Arrival-Departure)
  - Poll Site Manager = $19.91 per hour (Arrival-Departure)
  - Board of Elections Technician = $25.75 per hour (Arrival-Departure)

<u>Board of Elections Service Fees:</u>

- Proofing Ballots = $77.02 per hour (est. ½ hour)
- Absentee Printing & Materials = $.50 per ballot
- Absentee Mailing Preparing = $23.17 per hour (est. 1 hour)
- Absentee Mailing Postage = $.63 per ballot/envelope (based on USPS current rates)
- Preparing Legal Ads = $30.40 per hour (est. 1 hour)
- Charge from Eagle News = $45.00 (Estimated)
- Electronic Pollbook Programming = $54.93 per hour (est. 3 ½ hours)
- Electronic Pollbook Setup = $54.93 per hour (est. 3 ½ hours)
- Recanvass = $77.02 per hour (est. 3 hours)
- Audit = $42.00 per hour (est. 1 hour)
- Certification = $30.40 per hour (est. 1 hour)

Option #3 - Village conducts their own election with their own materials and equipment.

BOE will provide lists to Villages, but we no longer will be loaning out election equipment. With the increased election processes and limited timelines, we can no longer take on the responsibilities of villages without compensation for our time as we have endured ample overtime hours. We have also invested a great deal time and funds into improving our election processes with new voting equipment.

Dustin M. Czarny
Commissioner (D)
Onondaga County Board of Elections

Kevin P. Ryan
Commissioner (R)
Onondaga County Board of Elections

New York State Board of Elections

Cyber Security Regulation Compliance Certification Checklist

For each of the Cyber Security Regulation elements listed below, please provide current compliance Status (via Yes/No dropdown selection) and provide any additional information required as shown.
For any questions or assistance, please contact the Secure Elections Center at Secure@Elections.NY.Gov or (518) 473-4803

6220.2 Cyber Security Program		Status	Additional Actions/Information Required
(e)	Establish Agreement with IT Director, the head of the County IT Department or a contracted Managed Service Provider	Yes	

6220.3 Cyber Security Program Requirements		Status	Additional Actions/Information Required
(a)(1)	Data Classification	Yes	
(a)(2)	Asset Inventory	No	Please complete an entry on the Compliance Plan tab for this item, 6220.3(a)(2)
(a)(3)	Patch Management	No	Please complete an entry on the Compliance Plan tab for this item, 6220.3(a)(3) Per 6220.3(a)(3)(v), please also provide documentation for any technology unable to be updated or patched.
(a)(4)	Vulnerability Scanning	Yes	
(a)(5)	Backups of Election Data	Yes	
(a)(6)	Restoration of Data	Yes	
(a)(7)	Network Segmentation	No	Please complete an entry on the Compliance Plan tab for this item, 6220.3(a)(7) Per 6220.3(a)(7)(iv), please also provide documentation for any communications to information systems unrelated to Elections. Per 6220.3(a)(7)(xvi), please also provide documentation for any workstation macros or browser extensions. Per 6220.3(a)(7)(xix), please also provide documentation for any exceptions to Baseline image.
(a)(8)	Remote Access	Yes	
(a)(9)	Logging	No	Please complete an entry on the Compliance Plan tab for this item, 6220.3(a)(9)
(a)(10)	Incident Response	Yes	Per 6220.3(a)(10)(iii), please also submit copy of updated Incident Response Contact List.
(a)(11)	Continuity of Operations	Yes	Per 6220.3(a)(11)(iii), please also submit copy of CBOE Continuity of Operations Plan to State Board.
(a)(12)	Credential Management and Access	No	Please complete an entry on the Compliance Plan tab for this item, 6220.3(a)(12) Per 6220.3(a)(12)(ii), please also provide documentation for any information system unable to accommodate password requirements. Per 6220.3(a)(12)(iv), please also provide documentation for any information system unable to accommodate unique credentials.
(a)(13)	Multi-factor Authentication	No	Please complete an entry on the Compliance Plan tab for this item, 6220.3(a)(13) Per 6220.3(a)(13)(iv), please also provide documentation for any information system that does not support multifactor authentication.
(a)(14)	Email and Web Protections	No	Please complete an entry on the Compliance Plan tab for this item, 6220.3(a)(14)
(a)(15)	Third Party Risk Management	Yes	
(a)(16)	Continuous Monitoring and Reporting	Yes	
(a)(17)	Removable Media	Yes	
(a)(18)	Security Awareness Training	No	Please complete an entry on the Compliance Plan tab for this item, 6220.3(a)(18)
(a)(19)	Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)	Yes	

6220.2 Cyber Security Program, cont.

Per 6220.2, we certify:

(a) Establishment of a cyber security program that includes all of the elements required under section 6220.3 of this part to ensure the protection and safety of all systems and machines that access, store, process, and transmit election data, other than voting systems which already have security protocols pursuant to section 6210.11 of this part.

(b) Compliance of this cyber security program to the State Board of Elections annually but no later than August 1st in any given year.

(c) We have successfully established each element outlined in section 6220.3 of this part, or, in the alternative, submitted a plan for compliance to the State Board of Elections that includes a target completion date for any outstanding elements.

(d) Designation of two, bi-partisan Elections System Security Officers (ESSOs) to the Secure Elections Center in a letter to the Co-Executive Directors of the State Board of Elections signed by both County Commissioners, who are:

(1) responsible for the establishment of the cyber security program,

(2) designated as the points of contact with regard to the board of elections cyber security program, and in addition but not limited to, emergency response, incident communications, and recovery of election operations.

County: Onondaga

ESSO 1:

Name: Kevin Sexton

Title: Chief Information Officer

Email: kevinsexton@ongov.net

Phone: (315) - 435 - 8339

Commissioner 1:

Name: Dustin M. Czarny

Title: Democratic Commissioner

Email: dustinczarny@ongov.net

Phone: (315) - 383 - 4318

Date: 7-31-25

Signature:

Comments:

ESSO 2:

Name: Mitch Edwards

Title: Office Auto Analyst

Email: mitchedwards@ongov.net

Phone: (315) - 435 - 4707

Commissioner 2:

Name: Kevin P. Ryan

Title: Republican Commissioner

Email: kevinryan@ongov.net

Phone: (315) - 427 - 1923

Date: 7/31/25

Signature:

Comments: