Disposal of Election Equipment

The chain of custody of election equipment should be maintained from acceptance to proper disposal. If election equipment falls into the wrong hands, it not only jeopardizes the security and integrity of the jurisdiction that owned the equipment; it jeopardizes every other election jurisdiction that uses similar systems. In addition, even if the person or entity who improperly acquired the equipment does not maliciously exploit the data, a break in the chain of custody of election equipment can undermine faith in the integrity of the entire electoral system. As election jurisdictions procure new election technologies, they will often need to dispose of outdated election equipment. This document provides guidance and best practices election officials should take prior to the disposal, sale, transfer, or destruction of election equipment.

DISCLAIMER

The guidance and best practices contained in this document are for informational purposes only. Jurisdictions should consult their legal representatives to ensure all legal and contractual obligations are met prior to the disposal, sale, or destruction of election equipment.

There are security risks associated with the disposal, sale, or destruction of computer equipment and storage devices. Election officials must practice due diligence to properly account for all election equipment in their inventory. All election offices should develop a Security Plan or Incident Response Plan to monitor, detect, respond to, and mitigate incidents, such as a break in the chain of custody of equipment in their inventory, should they occur. Many states have statutory or regulatory requirements for county election offices to develop and update security chain of custody plans. Additionally, states may require emergency response continuity of operations plans. The EAC provides a variety of resources for Election Security Preparedness.[1] The Cybersecurity and Infrastructure Security Agency (CISA) Cyber Incident Detection and Notification Planning Guide for Election Security provides guidance for developing a basic cyber incident response plan.[2] The Department of Homeland Security's Incident Handling Overview for Election Officials provides guidance on steps for handling cyber incidents.[3] Although both guides focus on cyber incidents, the principles apply broadly to incidence response readiness.

Before disposing of, selling, or destroying any voting equipment or election technology, election officials should work with their Information Technology/Information Security support team to ensure that all necessary back-ups are made, and procedures are followed, and they comply with all laws and contractual obligations.

Chain of Custody and Inventory Control

It is critical to maintain a complete and accurate inventory of all election equipment, including ballot scanners and tabulators, ballot marking devices, communication equipment, supervisor or administrator devices such as smart cards, servers and workstations, and removable storage media. Prior to disposing of any election equipment, election officials should ensure they have a complete inventory of all election equipment. This inventory should contain at a minimum:

[1] See:https://www.eac.gov/election-officials/election-security-preparedness (accessed Feb. 28, 2023)
[2] See: https://www.cisa.gov/sites/default/files/publications/cyber-incident-detection-and-notification-planning-guide-for-election-security-508_1.pdf (accessed Feb. 28, 2023)
[3] See: https://www.cisa.gov/sites/default/files/publications/incident_handling_elections_final_508.pdf (accessed Feb. 28, 2023)

- Equipment – maintain a list of equipment, serial numbers, and quantity in each physical location, such as the election office, warehouse or storage facility.
- Machine Checkout – inventory control should track equipment when it is (1) being released and returned for an election, (2) released and returned for a demonstration, and (3) accepted from or returned to the vendor for maintenance or repair.
- Usage History – maintain a history of elections for which each piece of equipment has been tested and used.
- Maintenance History – maintain a history of routine or preventive maintenance tasks completed on each individual device.
- Repair History – maintain a history of repairs to individual devices.
- Disposal – maintain a history of disposal for each device that includes (1) the entity or persons, method, and date when data was wiped from the device, (2) who oversaw each step in the disposal process, and (3) a record of each disposed device with the date of disposal, how it was disposed and who authorized the disposition.

Disposal and Destruction of Election Equipment

Prior to the disposal of any voting system, all equipment should be sanitized, which is the process of removing all data from a device. Solely deleting the files on the device is not sufficient as it does not remove the files from memory. Deleted files remain on the device and can still be recovered. Therefore, all equipment should be taken back to the condition of a non-functioning piece of hardware with no software or firmware remaining on the equipment. For more detailed information on determining how to sanitize election technology, see the Clearing and Sanitization Matrix from Defense Security Service in NIST Special Publication 800-88 Revision 1.[4]

Election officials must practice due diligence to properly sanitize and dispose of election equipment. This involves at a minimum:

1. Determining if their Information Technology/Information Security support team has a process for wiping data from memory before disposing of or selling equipment. Election officials should follow all requirements set forth by their jurisdiction.

   For computer equipment, there are tools that overwrite every sector of a hard drive multiple times that meet the Department of Defense security standards for wiping data (DOD 5220.22-M, Data Wipe Method).

2. Confirming the destruction and disposal process with their voting system manufacturer (vendor) to make sure it is sufficient for meeting the requirements of the technology and equipment to which it is applied. If replacing old equipment with new equipment from the same vendor, consider including a requirement in the contract that the vendor take back the old equipment.

3. Verifying there are no legal or contractual obligations that must be met before disposing of or selling any of the election equipment.

A jurisdiction may determine that it would be best to outsource the destruction and disposal of the election equipment. When utilizing this option, it is recommended that the jurisdiction exercise due diligence, including only using a disposal company that is certified by a recognized trade association or similar third party. Also, the jurisdiction should require a certificate of destruction stating that all data stored on the election equipment has been properly wiped and all hardware has been appropriately discarded. There may be local or state laws concerning electronic waste disposal and environmental or public health hazards.

[4] See: https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final (accessed Feb. 28, 2023)

Voting Technology Purchased with HAVA Funds

Equipment purchased with Help America Vote Act (HAVA) funds can be disposed of either collectively as a system or individually as components, as long as it meets the guidelines outlined in Common Rule requirements for disposition of equipment purchased with federal funds (41 CFR 105-71.132 or 2 CFR 200.313).

Items of equipment with a current per-unit fair market value in excess of $5,000 may be sold with the funds credited to the state/local HAVA election accounts in an amount calculated by multiplying the current market value or proceeds from sale by the HAVA (Federal and Matching Funds) share in the cost of the equipment.

In cases where the titleholder fails to take appropriate disposition actions, the EAC retains the right to direct states to take excess and disposition actions.

States and local jurisdictions can continue to use equipment purchased with HAVA funds for its original purpose for as long as needed, even if the EAC award used to purchase the equipment has been closed. Equipment may also be used for other federally supported activities currently or previously funded by a federal agency. Additionally, equipment can be traded-in for replacement equipment for same purposes.

Without prior approval from the EAC, equipment purchased with HAVA funds with a current per unit fair market value of less than $5,000, may be traded-in, sold or scrapped on an as-needed basis with no further obligation to the EAC beyond recording disposition in the appropriate equipment inventory log.

The final record retention period for equipment replacement or disposition begins on the date the State submits its final Federal Financial Report (FFR) to the EAC and continues for three years. For equipment replacement or disposal after the end of award period, the three-year record retention period begins from the time the equipment is traded-in or disposed of and continues for three additional years.

For more information about disposal, sale or destruction of election equipment purchased with HAVA funds, contact the Office of Grants Management at: havafunding@eac.gov.

Election Equipment Disposal Checklist

Document each piece of equipment in your inventory. This documentation should include the following:	
• The type of equipment being inventoried. Include the make, model, and serial number, if available. Include removable storage media.	☐
• A record of all security mechanisms or seal numbers applied to each piece of equipment. Verify that any seals or other security mechanisms are intact.	☐
• A detailed record of check-out, usage, maintenance, and repair history.	☐
• The physical location of the equipment, such as an elections office, warehouse, or other storage facility. Include documentation about the access controls in place at each storage facility, including a list of individuals who are authorized to access each facility.	☐
Confirm all legal and contractual obligations prior to the disposal, sale, or destruction of any equipment. This should include the following:	
• Check with the voting system manufacturer (vendor) to ensure there are no contractual obligations that must be met.	☐
• Check with your legal representatives to ensure there are no legal obligations that must be met, including state and local laws and HAVA funding requirements, if applicable. If selling the equipment to another jurisdiction, check the terms of the sale and verify what is included in that sale (e.g. ancillary equipment).	☐
• If outsourcing the destruction or disposal of equipment, check the credentials of the disposal company and require a certificate of destruction.	☐
Document the chain of custody for the disposal, sale, or destruction of all equipment. This documentation should include the following:	
• Who will be receiving the equipment (often a voting system vendor).	☐
• Any additional parties that may be involved in the disposal, sale, or destruction of the equipment (such as the waste disposal or recycling facility).	☐
• Who oversaw each step of the process, including the individuals involved in wiping data from the equipment.	☐
• What equipment was sold, disposed of, or destroyed, as well as the methods used to wipe data from the equipment, the date and who authorized it.	☐