STATE OF COLORADO
Department of State

1700 Broadway
Suite 550
Denver, CO 80290

Jena Griswold
Secretary of State

Fact Sheet: 2024 General Election

Colorado's elections are protected by multiple layers of physical and network security measures designed to prevent unauthorized access and ensure accurate vote counts. The Colorado Department of State (CDOS) confirms that the November 5, 2024 General Election was secure and accurate, despite the posting of BIOS passwords for some voting equipment.

Passwords on affected active machines were changed. A thorough review conducted by Colorado Department of State staff determined there was no evidence of unauthorized equipment access. All BIOS settings were verified on active voting equipment affected by the password posting. For equipment that allowed for it, a hash value analysis was conducted, which further indicated no changes had been made to the system. The Department of State reviewed access logs for the 34 affected counties – no evidence of unauthorized access was discovered in that review.

Ballots were counted according to voter intent and tabulating equipment worked correctly—this was conclusively verified through Colorado's nation-leading bipartisan election audit. The risk-limiting audit established a statistical level of certainty that ballots were counted according to voters' intent and tabulating equipment worked correctly. Sixty-five contests were audited– two statewide contests, and one contest in 63 counties – and every audit showed at a 97% rate of statistical certainty that voting tabulation equipment worked correctly.

Multiple Layers of Security

Colorado's elections are protected by overlapping security measures. The following explains the multiple layers of physical and network election security:

- **Password Protections:**
  - There are two different passwords to all tabulation voting equipment components: a BIOS password maintained by civil servants at CDOS and an operating system password maintained by the County Clerk's offices.
  - Passwords require physical, in-person access to be used on voting equipment.

- **Physical Security Measures:**
  - Voting equipment is required to be stored in secure rooms that require a secure ID badge to access.
  - Entry is logged in an access log, which tracks who enters a secure area and when.
  - Voting equipment is under 24/7 video surveillance.

- **Strict Access Controls:**
    - Only specific background-checked individuals who have ID badges may access voting equipment.
    - All voting equipment is subject to strict chain-of-custody requirements, which track who is in possession of the equipment and when.
    - It is felony to access voting equipment without authorization.

- **Access Logs**
    - Access to voting equipment is tracked in access logs of who enters a secure area and when.

- **Hash Value Analysis**
    - For equipment that allowed for it, a hash value analysis was conducted, which further indicated no changes had been made to the equipment.
    - A hash value is a unique number that is altered when an applicable file is changed.

- **Paper Ballots**
    - Colorado has paper ballots that exist as an election record.
    - Paper ballots are audited during the Risk Limiting Audit to verify that ballots are counted according to voter intent and tabulating equipment works correctly.

- **Bipartisan Risk-Limiting Audits (RLA):**
    - Colorado was the first state to implement a statewide RLA in 2017, which establishes a statistical level of certainty that ballots are counted according to voters' intent and tabulating equipment works correctly.

- **Decentralized Vote Counting:**
    - Votes are counted independently in each county and then the results are aggregated.

- **Closed Network Voting System Components:**
    - Voting equipment is not connected to the internet.
    - Each county's voting equipment is segregated from all other counties'.

- **Risk and Vulnerability Assessments:**
    - CDOS conducts risk and vulnerability assessments, including penetration tests and external testing, with the U.S. Department of Homeland Security to check for vulnerabilities.
    - In August 2024, the Department of Homeland Security tested for internal and external vulnerabilities. These passwords were not discovered.
    - CDOS's external website systems are scanned for vulnerabilities by a third-party service. These passwords were not discovered.

- **Staff Training:**
    - All employees are required to take annual cybersecurity trainings on password strength, phishing, and other topics.

Timeline of Resolution of Password Posting

October 24, 2024:

- CDOS became aware that a spreadsheet with hidden passwords had been posted on a subpage of the department's website. CDOS did not initially know whether the passwords were active.
- CDOS immediately removed the spreadsheet from the website.
- CDOS consulted with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, as well as Dominion Voting Systems.
- CDOS determined that the passwords did not pose an immediate security threat.
- CDOS began a thorough assessment of how many, if any, of the passwords were in use for the over 2,100 voting components across the state.

October 25- 28:

- CDOS started to examine web traffic to the subpage and investigate whether there were signs of these passwords or anything related to them elsewhere on the internet or dark web.
- CDOS determined that 34 of Colorado's 64 counties were affected by the posting.
- CDOS worked to determine the size and scope of the issue to inform the technical and outreach plan before sharing it, to avoid fueling the major disinformation environment that surrounds elections.

October 29:

- CDOS completed the identification of the specific voting system components affected by the posting on the morning of October 29th. Department staff immediately began changing passwords. County Clerks were informed that day.

October 30:

- Department staff continued changing passwords.
- Governor Polis offers resources.

October 31:

- By the end of Thursday, October 31, all affected active equipment had undergone password updates with support from the Governor's Office of Information Technology and Colorado Bureau of Investigation.
- It was also confirmed that relevant equipment settings were correct for impacted active voting equipment.

November 1:

- The Denver District Attorney opened an investigation into the staff's posting of the spreadsheet that included the passwords.
- The Department of State is supporting and working closely with the Denver District Attorney's Office in that investigation

November 4:

- CDOS announces it is engaging a well-regarded law firm to conduct an outside investigation into the event, determining how it happened, how it could be prevented in the future, and any recommendations for improvement of practices and procedures.

November 4-5:

- Denver District Court reviewed the steps CDOS took to address the password disclosure.
- The District Court found CDOS acted independently to address the password posting and ensure the security of election systems, and found that Department staff and the Secretary of State took proper action to uphold their duties under the law.

November 8-12:

- The case was appealed to the Colorado Supreme Court on November 8. The Colorado Supreme Court declined to review the case on November 12.

November 21:

- Colorado's bipartisan Risk-Limiting Audit was completed.
- The risk-limiting audit confirms that ballots were counted in the way voters intended and tabulating equipment worked correctly.

November 27:

- The canvass in all of Colorado's 64 counties was completed, and each county canvass board approved the final tally of ballots cast and tabulated.

December 5:

- Secretary Griswold announced that the mandatory recounts of Colorado's State House Districts 16 and 19 are complete.

December 6:

- Secretary Griswold certified the 2024 General Election.
- Secretary Griswold and Governor Polis signed the certificates of ascertainment and the certificates of election for the U.S. House of Representatives.

December 9

- Baird Quinn LLC's report of their independent investigation is issued.

December 20

- Assigned additional cybersecurity training for all staff, including password management and security procedures, must be completed by December 20th.