AUDIT REPORT

Election Department
Electronic Poll Book and Voter
Registration Applications Audit

April 2021

CLARK COUNTY *Nevada*

Audit Department
Angela M. Darragh, CPA, CISA, CFE
Audit Director
countyauditor@clarkcountynv.gov

Audit Team

Angela Darragh, Director
Cynthia Birney, Audit Manager
Felix Luna, Principal Auditor
Chris Hui, Information Systems Auditor

Audit Committee

Commissioner Michael Naft
Commissioner William McCurdy II
Commissioner Ross Miller

About the Audit Department

The Audit Department is an independent Department of Clark County reporting directly to the County Manager. The Audit Department promotes economical, efficient, and effective operations and combats fraud, waste, and abuse by providing management with independent and objective evaluations of operations. The Department also helps keep the public informed about the quality of Clark County Management through audit reports.

You can obtain copies of this report by contacting us:

Clark County Audit Department
PO Box 551120
Las Vegas, NV 89155-1120
(702) 455-3269

CountyAuditor@ClarkCountyNV.gov

Or download and view an electronic copy by visiting our website at:

https://www.clarkcountynv.gov/audit/Pages/AuditReports.aspx

Contents

Background

The Clark County Election Department is responsible for planning, preparing, and conducting all federal, state, and municipal elections in Clark County. This includes elections in unincorporated Clark County, City of Las Vegas, City of Henderson, Boulder City, City of Mesquite and City of North Las Vegas.

The Election Department monitors every aspect of voting, including candidate filing, registering voters, printing ballots, maintaining voting machines, recruiting volunteers, training volunteers, and tabulating ballots. They also handle petition processing and manage electronic poll books for each election. The Department provides an Early Voting Program and administers absentee/mail ballet voting in an effort to make voting more accessible. Lastly, the Department is responsible for coordinating early voting and election day vote centers.

The Department handles both the general and primary elections. The general election is held on the first Tuesday after the first Monday of November in each even-numbered year and the primary election is held on the second Tuesday in June of each even-numbered year.

Electronic Poll Books Rolled Out Countywide in 2018

In 2018, the Department implemented electronic pollbook kiosks. These kiosks replaced traditional paper rosters at all voting sites. The kiosks allowed for the implementation of voting centers on Election Day, instead of traditional precinct-based polling places. The electronic pollbook kiosk allows poll workers at any site to look up and process any Clark County registered voter, no matter where they live or what their assigned precinct is. Exhibit 1 shows voters in Clark County using electronic poll books at a voting center.

Exhibit 1: Voters and Poll Workers in Clark County Using Electronic Poll Books

Source: Bridget Bennett/Bloomberg via Getty Images

During the 2019 Municipal General Elections, there were 976,489 registered voters. A total of 22,257 register voters voted in the election, including 6,591 who voted on election day, 12,253 early voters submitting votes at one of 23 early voting locations, and 3,413 voters submitting mail-in-ballots.

Voter turnout is significantly higher during general elections. In the 2018 General Election, 654,919 out of 1,096,866 registered voters voted. A total of 223,188 voted on election day, 382,659 voted during early voting, and 49,072 submitted mail-in-ballots.

Clark County Election Department's Voter Roll Contains Nearly 71% of all Registered Voters in Nevada

As of May 2020, there are 1,331,067 registered voters in Clark County. All in all, the Clark County Election Department's voter roll contains nearly 71% of all registered voters in Nevada (*based on statistics from the Nevada Secretary of State which reports 1,876,168 total voters in Nevada.*)

The Election Department reports having approximately 1,300 electronic poll book kiosks as of 2019. The kiosks utilize a comprehensive software and hardware package that allows for the retrieval of voter records, confirmation of the voter's status, precinct, ballot style and other general functions. The kiosks are used at all early voting and election day voting centers to interface with the Department's voter registration database.

The electronic poll book software, voter registration data management system and poll book hardware are all part of the Department's election management system. This system is supported by Votec Corporation, a third-party vendor. The most recent contract with Votec was approved February 4, 2020 and has an estimated value of $5,548,050 should all renewal options and increased user requirements be exercised.

We conducted this audit due to cybersecurity concerns that have arisen in recent years, as mentioned in the October 8, 2019 Governing Magazine article, Cybersecurity and Democracy Collide: Locking Down Elections:

> *"Presidential campaigns are now underway, and election systems are still vulnerable. From voter registration databases to result-reporting websites to the voting machines themselves, researchers have identified soft spots across the system for hackers to exploit, meaning cybersecurity is now a front line of defense for American democracy."*

> *"In a briefing before senators in August 2018, then-DHS Undersecretary for the National Protection and Programs Division Chris Krebs said top vulnerabilities included the administration of voter registration databases and the tabulation of data, the former being easier to attack."*

> *"…components most in need of immediate cybersecurity fixes were voter registration databases, and election-night reporting websites run by the states – again, to prevent hacks that wouldn't affect vote tallies but might cause confusion."*

Strong Controls Over Electronic Poll Books and Voter Registration Systems is Crucial in Today's Environment

Proper controls over electronic poll books and voter registration applications is critical for maintaining the integrity of elections in Clark County. In addition, proper controls ensure the availability, reliability and confidentiality of the information stored in these applications. Lastly, strong controls are crucial in an environment that has seen increased cyber security threats to all elections systems across the country, including voter registration databases.

Scope and Objectives

The objectives of this audit were to:

- Examine the Election Department's electronic poll book and voter registration applications for data

---

integrity, availability, and confidentiality. Specifically focusing on the Votec Election Management and Compliance System (VEMACS), PollPower, the voter registration system and VoteSafe, the electronic poll book management application.

- Review compliance with applicable Nevada Revised Statutes pertaining to elections.

Our procedures considered the period of March 2018 through January 2020. The last day of fieldwork was May 8, 2020.

An additional objective was added after the November 2020 General Election:

- Examine the mail ballot counting process for reasonableness.

We performed procedures on November 5, 2020. The last day of fieldwork was January 6, 2021.

Methodology

To accomplish our objectives, we conducted a preliminary survey that included reviewing applicable policies, procedures, and statutes. We interviewed staff and performed a walkthrough observation of various areas to identify key operations. Based on the risks identified during our preliminary survey and discussions with staff, we developed an audit program. We then performed the following testing procedures:

- Reviewed documentation supporting the existence of business continuity and disaster recovery plans to evaluate the plans' comprehensiveness and effectiveness.

- Reviewed documentation evidencing the periodic training of key staff on the business continuity plan and disaster recovery plans.

- Obtained a current inventory of computer hardware and selected samples (*laptops, desktop computers and servers*) based on auditor judgment to verify their existence by tracing to the last known location.

- Confirmed timely implementation of application patches and reviewed patch management practices through inquiry with staff and verification of software versions to determine compliance with best practices.

- Verified that equipment disposal procedures are in accordance with Information Technology Directive 1 through inquiry with Election staff and County IT staff as well as reviewing disposal procedures.

- Used statistical sampling to select a sample of 71 poll-workers (*out of 3,237*), to confirm that the appropriate training was provided by comparing the worker's job description with the training class taken and confirming that the worker's signature, per the class sign-in sheet, agreed to the voter registration database. Also verifying that the sampled worker passed the training class, by reviewing documented test scores.

- Determined whether background checks were done for all employees and volunteer poll workers, by requesting evidence that a background check was conducted.

- Verified that poll workers are not related to a candidate for nomination or election, by attempting to review the poll workers' signed affidavits and any other supporting documentation.

- Tested system ballot mapping, as of July 2019, to determine if voter precincts and districts are correct based on the address entered, by statistically selecting a sample of 71 out of 1,243,724 active and inactive registered voters and cross referencing their address to precinct maps to verify if the ballot style in the voter registration system is correct.

- Reviewed user access and permissions on 10 PollPower users, 15 VEMACS users and all database users to determine whether they have appropriate permissions based on their job duties and verify whether the user activities log is being reviewed for those systems, in accordance with best practice.

- Verified that the voter registration database is being periodically maintained with information provided by the Secretary of the State by cross referencing reports that are on the Secretary of the State portal with the current database ensuring any discrepancies are either resolved or being investigated by the Election Department.

- Verified that the voter registration database login-logout and failed login attempt logs are being periodically reviewed, through inquiry with staff and review of IT documentation.

- Verified that the voter registration database is being backed up at least annually, that the backup is regularly tested and that any backups are stored in a secure location through inquiry with staff and review of IT documentation.

- Verified that encryption is used on the voter registration data that is transmitted and stored through inquiry with staff and review of IT documentation.

- Verified that passwords for the election management applications are established in accordance with County IT Directives by reviewing evidence of the application's password configuration and parameters of failed password setups.

- Determined if results from third party security tests were implemented and resolved through inquiry with staff and review of IT documentation.

- Reviewed documentation pertaining to patch management for the VEMACS and PollPower applications to determine adherence to best practices.

- Verified that mail ballots are secured, tracked, and counted.

- Verified that mail ballot process and procedures follow Nevada Revised Statues.

While we did not perform detailed testing on the mail ballot counting processes, we believe making inquiries, observations and examining documents was sufficient to evaluate processes for material weaknesses or significant deficiencies.

Furthermore, while some samples selected were not statistically relevant, we believe they are sufficient to provide findings for the population as a whole.

Our review included an assessment of internal controls in the audited areas. Any significant findings related to internal control are included in the detailed results.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained

provides a reasonable basis for our findings and conclusions based on our audit objectives. Our Department is independent per the GAGAS requirements for internal auditors.

Conclusions

Overall, we believe the Clark County Election Department adequately maintains the integrity, availability, and confidentiality of the data within the electronic pollbook and voter registration database.   In addition, we believe processes and procedures in place for processing mail ballots mitigate errors and fraud and ensure the security, integrity, accuracy, and confidentiality of the mail ballot count process. However, we did identify some concerns and opportunities for improvements. These include:

- Shared application credentials;
- Opportunities to improve logical controls;
- Policy and procedures pertaining to poll worker applications, training and NRS 293.217 that should be created or revised;
- Background checks on certain employees that should be considered;
- Opportunities to improve various IT controls;
- Walk-in voter registration applications that should be tracked; and
- A voter registration list update that did not capture some necessary amendments nor has the process documented.

Each finding includes a ranking of risk based on the risk assessment that takes into consideration the circumstances of the current condition including compensating controls and the potential impact on reputation and customer confidence, safety and health, finances, productivity, and the possibility of fines or legal penalties.

Auditee responses were not audited, and the auditor expresses no opinion on those responses.

Findings, Recommendations, and Responses

Controls of Database User Credentials Could be Improved (High)

We found multiple staff members using the same login credentials. This practice differs from the U.S Election Assistance Commission checklist which states:

"The U.S Election Assistance Commission issued a checklist for the security of voter registration data on Oct 23, 2017 which notes:

Auditability - the database should have sufficient logging capabilities, including who has made modifications, the nature of the modifications, the authority to make those modifications, and to determine if there has been any unauthorized or inappropriate activity.

Additionally, the current practice of sharing user credentials is in violation to Clark County IT directives No.1, which states:

Generic and Guest Accounts: The use of generic and guest accounts is not permitted. Individuals who require access to County Computing Systems and Networks must be assigned and must use a unique User ID with limited permissions.

Overall, sharing credentials reduces accountability for changes to the database because changes cannot be attributed to a specific person. It also reduces the ability to determine if there is unauthorized activity, as noted by the U.S Election Assistance Commission.

Recommendation	1.1 Discontinue the use of the shared account and create separate accounts for each user.
Management Response	1. Need to confirm that the application allows for separate accounts. Moving to new version and will create separate accounts if the application allows it.

Improvements to Election Application's Logical controls (High)

We identified various concerns while testing logical controls for the VEMACS, PollPower and VoteSafe computer applications.

Upon notification of the concerns, the Election Department submitted a change request to rectify the concerns.

We did find that there are some system limitations for to correct some of the logical control concerns on the three systems.

While we acknowledge that there are some limitations to the system, we believe alternative controls can be put in place to mitigate the concerns.

Recommendation	2.1	Document and implement additional procedures to mitigate identified risks.

Management Response	1.	This is in process or completed.

Policies and Procedures for Poll Workers are Not Always Followed (High)

The Department uses volunteers and workers to act as election board officers in accordance with NRS 293.217(1) which states *"The County clerk of each county shall appoint registered voters to act as election board officers…"*

During our testing, we found that 3 of the 71 of sampled poll workers (*or 4.2% of 3,237 total poll workers for the audit period*) were not active registered voters.

To comply with NRS, the Election Department policies and procedures require that all poll workers to be registered to vote in Nevada. By not ensuring that all poll workers are registered voters, the Election Department is not complying with their policies and procedures and reduce their compliance with NRS.

We found that the training class sign in sheets, indicating that the poll workers were adequately trained, could not be located for 46 of the 71 *(64.8%)* sampled poll workers. We were informed that 3 of the 71 *(4.2%)* poll workers received one-on-one instruction and training; however, no documentation was available. Without documentation, we could not ascertain that sampled poll workers were adequately trained.

The Election Department policies and procedures require that all poll worker training documentation be retained. By not retaining this documentation, the Department is failing to comply with their policies and procedures. Further, this lack of documentation could make it difficult for a supervisor or reviewer to ascertain that Department procedures are being followed.

For the 2018 primary and general elections (including early voting), we requested and reviewed 71 class rosters. While Department policies and procedures require that class rosters include a participant grade of either pass 'P' or fail 'F' - none of the sampled class rosters included such markings.

We requested and reviewed 46 class rosters for the 2019 primary election (*including early voting*).One roster noted "P" in the P/F column for all attendees, while 15 rosters used a "√" next to the attendee's names to indicate they passed the course. Thirty class rosters had no P/F notation and one class roster sheet had an "F" in the P/F column for one attendee. *NOTE: That individual did not retake the training or*

work in the election. By not properly documenting participant grades, a Department reviewer will have difficulties asserting that all class participants received passing marks on their classes.

We found that the Recruiting manual used by recruiters is outdated with no documented revision date. The recruiters do not follow the procedures for poll worker applications received over the phone as they are currently listed in the manual. The policy states that the recruiter is to fill out the top portion of Poll Worker Application and write "registration sent today (date)" at the top when applications are received over the phone. The application is then to be placed in the New Applications basket for processing. Instead, staff now enter the information directly into VEMACS while they have the person on the phone to save time. This practice results in a deviation from established policies and procedures.

Recommendation	3.1	Update policies and procedures to reflect current procedures in place for poll worker applications received over the phone and grading and evaluating poll workers.
	3.2	Implement procedures to verify that all poll workers (except for students) are registered voters in compliance with NRS 293.217 and Departmental policy.
	3.3	Implement procedures to verify that the registration status for poll workers is active when working on an election.
	3.4	Train staff on procedures for documenting staff training.
	3.5	Implement procedures to retain class roster sign in sheets.
Management Response	1.	Change process for the intake of poll workers to include the confirmation of voter registration. Notify recruit of the requirement to be a registered voter and require them to submit a registration form at time of training if not registered. Add to sign in sheet to document registration at training.
	2.	After training, using sign in sheets, verify that those workers required to register did so at training.
	3.	Retain training sign in sheets that have been used to verify registration for auditing purposes after the election.
	4.	Document in training for recruiters and trainers the requirements for verifying voter registration.

5. Organize sign in sheets by date of training for later reference and maintain for 22 months.

Policies and Procedures Need to be Implemented to Ensure Compliance with NRS 293.217 (High)

Poll worker applications are entered into VEMACS, and then destroyed, as their user profile in VEMACS serves as the application record. On the application, applicants certify, by signature, that they are not a candidate for nomination or election nor that they are related to a candidate for nomination or election in accordance with NRS 293.217.

Since the original applications are not retained and VEMACS does not record the applicant's assertion, there is no way to confirm that the applicants did indeed provide the affirmations of candidacy and relationship.

We also found that poll workers do not submit new applications for every election. During recruitment, recruiters contact poll workers that are on the active poll worker listing to verify information on file and confirm participation. This is done over the telephone and poll workers re-certify verbally to not being a candidate or related to a candidate for nomination or election. For new applications received over the phone, the recruiter reads the certification requirements. However, there is no documentation to confirm that poll workers certified that they are not a candidate or related to a candidate for nomination or election.

By not keeping a record of the poll workers confirmation of candidacy and relationship, the Department may not be able to validate their efforts should there be a need. Further, the current procedures may create a lax environment where a poll worker is not inclined to reveal their candidacy or relationship to a candidate, potentially creating a conflict of interest during an election.

Recommendation

4.1 Develop, implement, and enforce policies and procedures pertaining to poll workers certifying, for every Election they serve in, that they are not a candidate or related to a candidate for nomination or election in compliance with NRS 293.217.

4.2 Develop, implement, and enforce policies and procedures for retention of poll worker certifications for periodic review.

Management Response

1. Add verification on training sign in sheet that indicates the worker has confirmed that they are not a candidate or related to a candidate in this election.

2. Retain sign in sheets and organize by date of training for auditing at a later date. Retain for 22 months after election.

3. Will be adding verification of these items to our Oath for all workers.

Background Checks Should be Performed for Poll Workers (High)

The Election Department does not conduct background checks on poll workers. While state statutes do not require a background check, some poll workers, specifically those who are Laptop Operators and Kiosk Specialists, are able to view confidential voter information, namely voter information that that is marked confidential and not normally included in public voter datasets. This includes voter information for high profile voters, elected officials, law enforcement officials and other voters who have marked their information confidential and not part of public datasets. Some minor adjustment to the data can be performed by these poll workers.

Voter's information marked confidential could become compromised by poll workers, which could potentially result in decreased confidence in the election process and decreased trust in Clark County Government's ability to protect voter's personal information. We believe that by implementing a background check, the Department will discourage or identify individuals that may have malicious intentions.

Recommendation

5.1 Consider implementing procedures to perform some form of background check on poll workers, specifically team leads during early voting.

Management Response

1. Submit a request in our next budget to include the cost for background checks for all team leaders during early voting. If approved, we can move forward with compliance on this issue. Election Day are county workers who are already subject to background checks upon hire, those who aren't county employees are early voting team leaders and if the budget request is approved, they will be in compliance with this finding.

2. Will need to determine if the background check will be limited to fingerprinting or a full background check. If a full background check is required, it will slow down our recruiting efforts and require us to start recruiting early voting TL's earlier than we currently do.

Registration List Maintenance Should be Verified and Written Policies and Procedures Documented (High)

The Election Department performs periodic maintenance of the VEMAC voter registration list using informational reports from the Electronic Registration Information Center (ERIC). During this list maintenance process, the election Department will cross-reference cross state reports, deceased voter reports and in-state duplicate voter reports with the current voter registration database. This process is done to enhance

the accuracy and integrity of the voter registration list. We identified two concerns as follows:

List Not Fully Updated in June 2018:
During our testing of the list maintenance performed in June of 2018 we found that 3 of 804 records *(0.4%)* from the deceased report, 9 of 859 records *(1%)* from the in-state duplicate report, 1 of 62 records *(1.6%)* from the cross-county duplicate reports, and 145 of 12,701 *(1.1%)* records from the cross-state duplicate report were not updated in the VEMAC registration list due to oversights in the update process.

If the updates are not fully completed, then there will be active registrations for people who are not actually eligible to vote. Failure to fully update the list increases the risk that a person who is not eligible to vote may use the active profile to cast a vote.

Policies and Procedures Not Documented:
While the voter registration list is periodically updated using reports from ERIC, there are no written policies and procedures in place to document the process. Without written policies and procedures, performance of the work may be delayed should current staff who perform this function leave the Department or become unavailable. Documenting this process will ensure uniformity and will aide in future staff members in performing this task.

Recommendation	6.1 The Election Department should perform a closing review of the ERIC reports after the list maintenance has been completed to ensure that no updates were overlooked.
	6.2 Adopt written policies and procedures related to the periodic maintenance of the VEMAC voter registration list.
Management Response	1. Create written policies for staff to perform a review/audit of ERIC voter roll maintenance. Perform review/audit after every ERIC process.
	2. Will make use of EPM wherever possible to document the completion of these tasks.

Hardware Disposal Procedures Should be Improved (Medium)

We found that during the most recent disposal of hardware, the Department did not fully adhere to County Information Technology Directive 1.

When applicable and possible to do so, we believe any hardware disposal should adhere to County Information Technology Directive 1.

Recommendation	7.1	Implement a procedure to dispose of hardware in accordance with Information Technology Directive 1.

Management Response	1.	IT support will adjust disposal practices to comply with Information Technology Directive 1.

Business Continuity Plan Testing and Training Needs to be Documented (Medium)

The Election Department informed us that they perform testing of the disaster recovery plan prior to every election. However, they do not maintain documentation confirming that the test was performed. There is also no documentation of any deficiencies noted during the tests and whether steps were taken to remedy any deficiencies (if applicable).

The Department also stated that training on the business contingency plan was done for some key staff members. However, not all key staff members mentioned within the plan have participated in training, and the Election Department did not maintain documentation to show training was completed for anyone that received training. Further, business contingency plan should be updated to reflect current processes.

Not documenting the results from the testing and training of the business contingency plan reduces the ability of an independent reviewer to confirm what was discussed or identify any weaknesses noted during the training and testing of the plans. The Election Department may benefit from documenting previous discussions related to the plan tests for the purpose training and plan improvement. Further, this documentation can serve as a training tool in case of staff turnover.

Recommendation

8.1 Provide Business Contingency plan training to key staff members.

8.2 Document results of the training and testing of the business contingency plan and disaster recovery plan.

8.3 Review and update the Business Contingency plan annually to reflect current procedures, with Registrar sign off once the update is complete.

Management Response

1. Document the training of employees related to the COOP plans and retain the documentation for review/audit at a later date. Results of training should also be documented to include those who were trained.

2. Complete all COOP updates prior to every election cycle.

3. Department Head to sign the completed COOP plans once completed.

Risk Assessment Should be Improved (Medium)

The Election Department performed a preliminary risk assessment; however, the risk assessment could be improved.

The current risk assessment could leave risks unmitigated and could prevent the Department from finding solutions to existing threats.

The United States Department of Homeland Security (DHS) offers a cybersecurity assessment tool for local election jurisdictions. The Election Department has not taken advantage of this tool. This tool includes risk and vulnerability assessment, remote penetration test, cyber resilience review, vulnerability scanning and other drills that could assist the Election Department in strengthening their cybersecurity defenses.

Furthermore, utilizing the DHS tools could lower the cost of third-party assessments such as vulnerability scans and penetration tests as well as add additional layers of defense in the overall voter registration and election systems.

Recommendation

9.1 Complete risk assessment at least annually and document results.

9.2 Work with Department of Homeland Security to implement their cybersecurity assessments.

Management Response

1. Risk assessments are currently being completed by our Central IT cyber security staff. Will document testing.

Patch Management Tracking Process Could be Improved (Medium)

The Election Department works directly with their software vendor for requesting software patches and updates to the voter registration software, the electronic pollbook software, and the kiosk management software. Software patches are quick software modifications that fix a piece of programming designed to resolve a functionality issue, improve security and/or add new features.

We found that the Election Department generally keeps the voter registration applications up to date with the latest software versions and application patches. However, documentation of software that is installed or omitted could be improved.

Tracking the patch notes and what versions were installed or omitted to critical systems could benefit the Election Department mitigate additional risks and vulnerabilities.

Recommendation

10.1 Improve patch management to track patches that were installed or omitted.

| | 10.2 | Document a fallback plan for VEMACS and PollPower if installation is corrupted or updates do not install correctly. |

Management Response

1. Require IT Support staff to document patch management to VoteSafe software and any other software support changes.

2. Review current documentation and update accordingly.

Improvement to Inventory Tracking Needed (Medium)

We tested the location of 15 computers on the Election Department's inventory listing. We found that there were some discrepancies between what was listed on the inventory listing and the location of the computers.

Part of the reason for the outdated list is because the Election Department is going through a large technology replacement project. Additionally, an inventory managing staff member recently left the Department. Nonetheless, we believe it is important that the Election Department maintain an accurate inventory listing to minimize lost data or recovery time for stolen hardware.

Recommendation

11.1 Update the master inventory list annually and verify the location of laptops, desktops and servers that may contain voter registration data.

Management Response

1. Current process includes the use of several applications to complete inventory, which has not worked well for us. We will need to look at the purchase and acquisition of a single complete software package to complete the task for the entire Department, including the warehouse.

Data Encryption is in Place but Could be Improved (Medium)

We found data encryption during transmission to be reasonable. However, data encryption at other stages can be improved. Data encryption is an IT security mechanism where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data appears scrambled or unreadable to a person or entity accessing without permission.

The U.S Election Assistance Commission recommends that encryption be used for both data at rest and in transit, including encryption of the database, servers, backups, and any files used for distribution.

Encrypting data at rest would provide an additional layer of security to confidential data such as the information protected by NRS 293.503(6) and NRS 293.558.

Recommendation 12.1 Implement end to end encryption of the database as recommended by the U.S. Election Assistance Commission.

Management Response 1. County IT will review options.