State of North Dakota

Voting Process Security Assessment

[2022 Report]

SECUREYETI

DOCUMENT REVISION HISTORY

VERSION	DATE	CHANGE DESCRIPTION
0.1	10/03/2022	Initial Draft
1.0	10/24/2022	Final Draft

CONTENTS

1 KEY PARTICIPANTS

OFFICE OF THE STATE AUDITOR

Joshua C. Gallion State Auditor	jcgallion@nd.gov (701) 328-4781
James Kary Systems Auditor	jkary@nd.gov (701) 328-2580

OFFICE OF THE SECRETARY OF STATE OF NORTH DAKOTA

Jim Silrum Deputy Secretary of State	jsilrum@nd.gov (701) 328-2900
Brian Newby Director, Elections Unit	bnewby@nd.gov (701) 328-2900
Lee Ann Oliver Elections Unit	loliver@nd.gov (701) 328-2900
Brian Nybakken Elections Unit	bnybakken@nd.gov (701) 328-2900

NORTH DAKOTA INFORMATION TECHNOLOGY (NDIT)

Jessica Newby Information Security Officer	jnewby@nd.gov (701) 328-3190
Ryan Kramer Enterprise IT Architect	rkramer@nd.gov (701) 328-3190

2 INTRODUCTION

This Security Assessment Report (SAR) contains the results of a review of voting processes in the state of North Dakota (ND). The process review took place from 05/16/2022 through 07/31/2022. This assessment focused on possible vulnerabilities or threats related to the voting process only; no technical testing was conducted. The assessment team did not validate technical controls or review technical configuration of any system involved in the voting process.

The objective of this assessment is to evaluate the security of the voting process by interviewing key personnel and stake holders, reviewing technical documentation, and observing representative models of the voting equipment used in the voting process. This report is a review of current processes and is not intended to validate or invalidate the outcome of previous elections.

2.1 PURPOSE

The purpose of this document is to provide the ND State Auditor's office with a risk assessment of the state's voting process based on information provided by the Office of the Secretary of State (SoS) and North Dakota Information Technology (NDIT).

2.2 SCOPE

Over the course of the assessment, the assessment team conducted two remote interview sessions with key SoS and NDIT election staff. The assessment team also reviewed documentation provided, conducted in-person interviews and physical inspection of voting machines located in the state capitol building in Bismarck, ND.

3 EXECUTIVE SUMMARY

Vulnerabilities exist in every system, universally. When determining risk associated with a particular vulnerability, the result of the analysis must reflect existing safeguards. These safeguards are the system of checks and balances that prevent an attacker from exploiting a given vulnerability. When asked to evaluate the process that empowers North Dakotans to maintain democracy in their state, the assessment team found an election system with comprehensive safeguards at all levels.

North Dakota is unique in that fact that it is the only state in the Union that does not require voters to register before participating in an election. Instead, it relies on state identification and residence requirements to verify a person's entitlement to vote. Any qualified person with a valid form of identification listed in NDCC § 16.1-01-04.1 is eligible to vote.

In 2020 the state implemented a new voting system to streamline tabulation and election management. This new system has key controls that protect the integrity of the voting process.

The process revolves around a Central Voter File, which is used to keep a record of voters in the state. This file is automatically populated with information from the Department of Transportation as well as Vital Records.

- Although enabled by digital technology, the paper ballot cast by a voter remains the single source of truth. Should the accuracy of a digital tabulation be questioned, the paper ballots are preserved and can be recounted if needed.
- To ensure no one has tampered with the software that operates the digital tabulators, the machines are tested publicly to verify system logic and accuracy. The USB drives that contain the software are physically secured behind locked panels until the close of the election to prevent tampering.
- The digital tabulation machines generate a physical record of the tabulated results. This physical record is available to political party representatives and is delivered alongside the digital results to the County Auditor. The physical record can be used to verify the digital results have not been modified in transit.
- PollPads are used at each polling location to check voters in and prevent them from casting multiple ballots. This system also enables election officials to verify that the number of ballots distributed by poll workers matches the number of votes recorded for a particular precinct.

The assessment team included these, and other controls, when analyzing risk determination in this report.

The assessment team was able to identify six vulnerabilities with possible threat scenarios and determined a risk score for each. No scenarios were determined to be critical, high, or medium risk. All were determined to be low risk.

CRITICAL	HIGH	MEDIUM	LOW	VERY LOW
0	0	0	6	0

Table 1 - Summary of Risk Determinations

Overall, each vulnerability discussed in this report has little likelihood of being exploited. Even so, if exploited, most of these vulnerabilities would not prove effective or efficient for the purposes of fraudulently Influencing a state election. While, still, highly unlikely, the vulnerability that could have the most impact would involve collusion.

Because of the numerous safeguards in place to protect election integrity, the most effective way to influence a state election in North Dakota would have to involve unprecedented collusion. Not only collusion between state and local election officials, but also local party leaders, and employees within North Dakota Information Technology. Absent this mass cooperation of people operating in secrecy, it remains unlikely that the results of an election in North Dakota would be fraudulently influenced.

4 OVERVIEW

North Dakota is the only state that does not require its citizens to register in order to cast a ballot. Any citizen of the state can participate in an election if they present qualifying identification and proof of entitlement at the polling place. All votes are cast with a paper ballot. This paper ballot serves as the official record of the vote cast.

Holistically, the voting process comprises several technical systems and is coordinated by the SoS. The actual execution of the election and all subsequent reporting is the responsibility of the Auditor for each county. The current voting process was approved by the ND Legislature in 2019 and implemented in June 2020. This new process introduced electronic poll books, ballot marking machines, new digital tabulators, and compatible software.

4.1 SYSTEMS

The following is a summary of the systems that support the voting process.

4.1.1 CENTRAL VOTER FILE (CVF)

The CVF is software developed, specifically, for administering elections in ND. The CVF is an electronic record of ND Voters. It is continually updated with data from the Department of Transportation and ND Vital Records. Any citizen issued an ND driver's license or a non-driver's ID is automatically recorded in the CVF with a name, address, and date of birth. The CVF is a part of ND's overall Election Management System (EMS).

4.1.2 ND VOTING INFORMATION AND CENTRAL ELECTION SYSTEM (ND VOICES)

ND VOICES is the EMS that maintains voter record integrity among the County Auditors and the SoS. It facilitates CVF records and ballot building for elections. Citizens can also interact with ND VOICES via a portal at https://vip.sos.nd.gov for voting information.

4.1.3 POLLPADS

PollPads are tablet computers with poll check-in software developed by KNOWiNK[1]. Before a poll worker will provide a ballot, a voter must present a qualifying ID for the PollPad to scan. The PollPad locates the voter's record in the CVF. If the poll worker can verify the veracity of the voter's entitlement, the poll worker will provide an appropriate ballot based on the voter's precinct. The PollPads are networked on a dedicated cellular VPN using Cradlepoint[2] technology.

[1] KNOWiNK is an election technology company based out of Saint Louis, MO.

[2] Cradlepoint is a company headquartered in Boise, ID that develops routers, gateways and software for Wireless Wide Area Network (WWAN) edge networking. These devices connect to the PollPad through Wi-Fi and sync to ND VOICES through private cellular networks,

4.1.4 DS200

Developed and produced by Election Systems & Software[3] (ESS), This medium-sized machine tabulates votes from marked paper ballots inserted by the voters. The machine cannot operate without a USB drive installed. The USBs used to run the tabulators are programmed for each election by the manufacturer and distributed to the County Auditors by the SoS. The DS200 also has basic quality control functionality. The display will present an error message for overvoting, crossover voting, and blank ballots. Successful ballots are tabulated and stored inside the unit until the polls close. Spoiled ballots stored in a separate bin and eventually returned to the county recorder. Once polls close, the machine produces chits with a record of all votes recorded for every contest on any ballot fed to the machine and the USB drive is removed.

4.1.5 DS450

This machine digitally tabulates votes and operates in the same manner as the DS200. While the DS200 is fed ballots one at a time by voters, the DS450's function is to rapidly tabulate votes from absentee ballots. The DS450 can scan 50 votes per minute.

4.1.6 EXPRESSVOTE

This, table-top, machine is a ballot marking device intended to enable voters with disabilities. The ExpressVote does not tabulate votes. It produces a human-readable, paper ballot to serve as the official record. A DS200 processes ExpressVote ballots in the same manor standard paper ballots are tabulated.

4.1.7 ELECTIONWARE COMPUTER

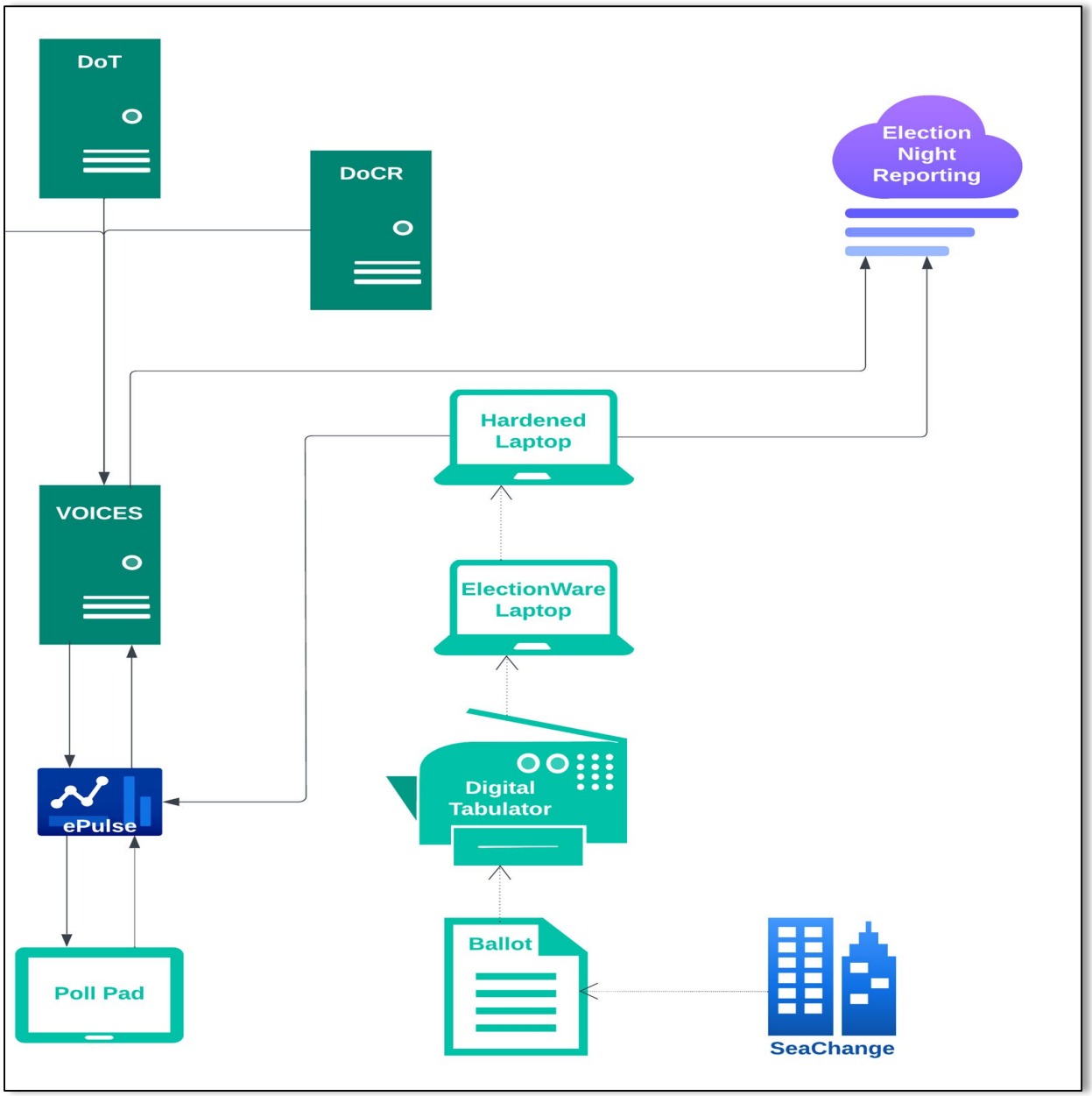
An air-gapped computer with limited functionality and ESS's ElectionWare installed. The County Auditor controls access to this computer and copies election results into the software from a tabulator's USB drive. The auditor can then produce reports from ElectionWare, copy them to a fresh USB drive, and take it to the hardened laptop.

4.1.8 HARDENED LAPTOP

A laptop with limited functionality that can connect to the NDIT's Virtual Private Network (VPN). With this laptop, the County Auditor can enter the results into the election database and the SoS's Election Night Reporting (ENR) Website.

[3] ESS designs and manufactures election systems. The company headquarters is in Omaha, NE.

4.1.9 ELECTION FLOW DIAGRAM



THE ABOVE DIAGRAM ILLUSTRATES THE RELATIONSHIP OF EACH PIECE OF THE EMS ALONG WITH THE PARTY THAT IS ULTIMATELY RESPONSIBLE FOR ITS MAINTENANCE & OPERATIONS.

4.2 SECURITY CONTROLS

Security Controls are safeguards designed to protect the confidentiality, integrity, and availability of a system or organization. The following is a summary of controls in place for the voting process.

4.2.1 CVF AND ND VOICES

This EMS has many functions. From an election security perspective, it is the system of record that keeps track of eligible voters, their polling place, and voting credit. ND VOICES is on a firewalled network and is monitored by NDIT and the Cybersecurity & Infrastructure Security Agency (CISA).

4.2.2 POLLPADS

PollPads are networked on a dedicated cellular VPN using Cradlepoint technology. Security profiles on these devices prevent them from connecting to any other network. PollPads sync with ND VOICES every two minutes. Once a voter is verified and checked in on a PollPad, that voter is not eligible to check in again at the same or another location. PollPads and ND VOICES are also used to verify how many ballots were cast at each polling location.

4.2.3 BALLOTS

The county is responsible for ordering, designing, and funding the ballots. They are specific to each precinct. The number of checked-in voters for each precinct should mirror the number of ballots cast in that precinct. The ballots are printed and designed by Seachange[4]. Ballot designs are not publicly released, and the tabulation machines are programmed for the specific image of the ballot. To make counterfeit ballots, a person would have to find the exact design, dimensions, and a way to print them. If all else fails, the physical ballots are the single source of truth, should the digital tally be compromised.

4.2.4 ABSENTEE BALLOTS

Voters can apply for absentee ballots, but the data on the application must match data in the CVF in order to receive a ballot. Absentee ballots are tabulated by election workers using the DS450. Ballots are sealed until tabulation.

Tabulation is overseen by an “Absentee Ballot Counting Board” appointed by the county auditor. The board consists of one independent representative to act as the inspector, and an equal number of representatives from each political party to serve as election judges. By design, there should always be non-partisan election workers and partisan election judges present when absentee ballots are unsealed.

In order to be counted, the signature on the back of the ballot-return envelope is verified against the signature on the absentee ballot application. If the signatures do not match, the voter is contacted, and must verify the signature with the same form of valid ID used in the application. Unverified ballots are not included in the final tally.

[4] Seachange is a printing company out of Minneapolis, MN with a specialty in election services and ballot printing.

4.2.5 DS200 AND DS450

These tabulation machines models are tested independently at a National Institute of Standards and Technology (NIST)-certified labs to meet the Voluntary Voting System Guidelines (VVSG) 1.0 baseline before they are sold to ND. Prior to an election, the machines are publicly tested for logic and accuracy as prescribed by the SoS. They are never connected to a network. Ports and ballot trays are locked during voting and cannot be accessed. The USB drives used to operate the machines must have the appropriate encryption key in order to operate the machine. After voting, the machine provides a receipt to the voter to verify the vote was counted.

4.2.6 CHITS

Chits printed by the tabulation machines contain a tally of the votes, are signed by election board members, and are available to election judges from all parties. They are also hand delivered, with the USB drive, to the County Auditor. The tallies on the chits can be verified against the number of voters checked into the polling location on the PollPad and the number of voters reported to the SoS database and ENR site. The tallies can also be checked against the report produced by the ElectionWare computer to verify integrity.

4.2.7 EXPRESSVOTE

Because the ExpressVote device does not tabulate votes, the paper ballot produced by the machine must be fed into a tabulation machine for the votes on the ballot to count. The voter can verify the ballot matches the voter's intention before feeding the ballot into the tabulator.

4.2.8 USB DRIVE

The encryption key that allows the USB drive to enable tabulator operation is known only to the manufacturer. These drives are programmed and shipped by the manufacturer, then distributed by the SoS. Election Board members hand deliver the drives from the polling locations to the County Auditor.

4.2.9 ELECTIONWARE COMPUTER

This is the only computer with the ability to decipher the vote tallies on the USB drives from the tabulators. This computer is programmed by the manufacturer specifically for each County Auditor and cannot be connected to a network by design. The ElectionWare computer is not used for general computing purposes. Its sole purpose is to compile vote tallies and produce reports. The County Auditor may designate a person as backup and grant privilege to access the computer, but access is limited.

4.2.10 HARDENED LAPTOP

By design, network capabilities on these laptops are restricted to a secure VPN operated and maintained by NDIT. They are not deigned to be used as general purposes computing workstation and have limited capabilities. These laptops have been configured with custom policies based on benchmarks published by the Center for Information Security (CIS-Benchmarks).

5 RISK METHODOLOGY

The following section details our NIST-based approach of calculating an overall blended risk score. This score is derived from a combination of overall impact, likelihood of attack initiation, likelihood of attack success, in addition to other surrounding factors or processes that would mitigate or intensifying risk.

5.1 RISK DETERMINATION

Risk calculation is determined by identifying a scenario in which the Voting Process could be threatened and performing a qualitative analysis of the impact and likelihood of that attack scenario.

- A threat is a circumstance or event with the potential to adversely impact the confidentiality, integrity, and/or availability of the Voting Process.
- Impact is the magnitude of harm that could be expected should a threat's potential be actualized.
- Likelihood is a weighted factor based on subjective analysis of the probability a threat's impact would be actualized. Likelihood analysis weighs difficulty of actualization, mitigating circumstances, and security controls in place. *(Likelihood of Initiation x Likelihood of Success)*

FIGURE 2 – RISK EQUATION

Impact and Likelihood are assigned severity ratings based on the analysis and risk is determined using the following table.

LIKELIHOOD \ IMPACT	Very Low	Low	Medium	High	Critical
Critical	Very Low	Low	Medium	High	Critical
High	Very Low	Low	Medium	High	Critical
Medium	Very Low	Low	Medium	Medium	High
Low	Very Low	Low	Low	Low	Medium
Very Low	Very Low	Very Low	Very Low	Low	Low

OVERALL RISK

Table 2 - Risk Determination Matrix

5.2 IMPACT SEVERITY RATINGS

IMPACT	
Critical	A threat has been **proven** to have been actualized and could be expected to have multiple severe or catastrophic adverse impacts on the confidentiality, integrity, and/or availability of the Voting Process
High	A threat could be **expected** to have a severe or catastrophic adverse impact on the confidentiality, integrity, and/or availability of the Voting Process
Medium	A threat could be **expected** to have a moderate adverse impact on the confidentiality, integrity, and/or availability of the Voting Process
Low	A threat could be **expected** to have a limited adverse impact on the confidentiality, integrity, and/or availability of the Voting Process
Very Low	A threat could be **expected** to have minimal to no adverse impact on the confidentiality, integrity, and/or availability of the Voting Process.

Table 3 - Impact Severity Ratings

5.3 LIKELIHOOD SEVERITY RATINGS

LIKELIHOOD	
Critical	If the threat is actualized, it is almost certain to have adverse impacts.
High	If the threat is actualized, it is highly likely to have adverse impacts
Medium	If the threat is actualized, it is somewhat likely to have adverse impacts
Low	If the threat is actualized, it is unlikely to have adverse impacts
Very Low	If the threat is actualized, it is highly unlikely to have adverse impacts.

Table 4 - Likelihood Severity Ratings

6 THREATS

Based on the process review conducted, the assessment team identified potential threats and then determined the associated risk for each.

6.1 KEY FINDINGS

#	Finding	Overall Risk
6.1.1	The Ability for a Voter to Cast Multiple Ballots	LOW
6.1.2	Identity Theft of Deceased Voters	LOW
6.1.3	Stuffing / Discarding Valid Absentee Ballots	LOW
6.1.4	Equipment Tampering (Tabulation Machine)	LOW
6.1.5	Equipment Tampering (USB Drive)	LOW
6.1.6	Absentee Ballot Fraud	LOW

6.1.1 THE ABILITY FOR A VOTER TO CAST MULTIPLE BALLOTS

OVERALL RISK: LOW

Perceived Threat:		Individuals could affect the outcome of an election by colluding and casting multiple ballots at different polling places.
Description:		Since it is possible for a voter to cast their in-person ballot at various locations within their county, a centralized system is required to track and record the issuance of ballots. The PollPad system is responsible for tracking the issuance of ballots received in-person. PollPads check the CVF in real-time to verify if a voter is eligible to receive a ballot for the current election. PollPads also update the CVF in order to accurately record when an in-person ballot is issued to a voter. Poll workers issue a ballot if the CVF indicates a voter does not have credit for receiving a ballot for the current election. Synchronization between each PollPad and the CVF occurs every two minutes, meaning end-to-end synchronization could take up to four minutes to complete. Once synchronized, a voter is credited with receiving a ballot in the CVF and would be ineligible to receive another. If multiple individuals fraudulently completed the PollPad verification process before the CVF and PollPads synchronize, all using the same identity, multiple ballots could be issued.
Impact:	HIGH	By casting enough fraudulent ballots to change the outcome of an election, the result of that election would not be valid. Any measure passed or candidate elected would have been done so illegally. This vulnerability would be expected to have a severe impact on the integrity of the election outcome. Should the fraud be discovered, it could also impact voter confidence.
Likelihood:	VERY LOW	In order to receive and cast multiple ballots using the same identity, all malicious voters would have to complete the PollPad verification process within the same four-minute synchronization window. The logistics and coordination needed to complete this verification process would be difficult. In addition to forging a person's identity (PII, Valid ID, & Signature), Malicious voters would have to anticipate line length and other factors outside of their control. The number of fraudulent votes cast per identity would be limited to the number of polling places in that person's county. Finally, post-election auditing would indicate multiple ballots were issued to the same individual. The voter's record would be flagged, and information would be turned over to the State Police for further investigation.

6.1.2 IDENTITY THEFT OF DECEASED VOTERS

OVERALL RISK: LOW

Perceived Threat:	Individuals could affect the outcome of an election by casting in-person or absentee ballots on behalf of deceased individuals.	
Description:	The CVF is database of all individuals who are currently eligible to vote. Both in-person and absentee ballots are only issued once eligibility has been confirmed with the CVF. Deceased persons are immediately removed from the CVF as soon as their death is reported by North Dakota's vital records. If there is a delay in reporting a person's death, an individual could impersonate and cast a ballot using the deceased individual's identity.	
Impact:	HIGH	By casting enough fraudulent ballots to change the outcome of an election, the result of that election would not be valid. Any measure passed or candidate elected would have been done so illegally. This vulnerability would be expected to have a severe impact on the integrity of the election outcome. Should the fraud be discovered, it could also impact voter confidence.
Likelihood:	VERY LOW	Although possible, the small time window to successfully exploit this vulnerability would greatly limit the number of fraudulent votes that could potentially be cast. In order to receive a fraudulent ballot on behalf of a deceased individual, the death must occur directly before the election, or the reporting of the death must be delayed. For in-person voting, the malicious voter would also have to impersonate the deceased and pass an identity verification process (PII, Valid ID, and Signature). Postmarks on absentee ballots would be checked against the CVF to verify the returned ballot was mailed before their death. Finally, post-election auditing would indicate that a vote was cast by a deceased individual. The voter's record would be flagged, and information would be turned over to the State Police for further investigation.

6.1.3 STUFFING / DISCARDING VALID ABSENTEE BALLOTS

OVERALL RISK: LOW

Perceived Threat:		Individuals could act or a group of individuals could collude to affect the outcome of an election by casting a bundle of pre-marked ballots. They could then discard valid absentee ballots to avoid detection.
Description:		Individuals or a group of individuals on the "Absentee Ballot Counting Board" could discard valid absentee ballots and replace them with pre-marked ballots supporting their chosen candidate or ballot measure.
Impact:	HIGH	Changing the outcome of an election by discarding valid absentee ballots and replacing them with fraudulent ballots would invalidate the results of that election. Any measure passed or candidate elected would have been done so illegally. This vulnerability would be expected to have a severe impact on the integrity of the election outcome. Should the fraud be discovered, it could also impact voter confidence.
Likelihood:	VERY LOW	The only opportunity a malicious individual would have to actualize this threat would be after absentee ballots are verified, but before they are tabulated. A malicious individual wishing to exploit this vulnerability would first have to have prior knowledge of the ballot design for one or more precincts to forge fraudulent ballots for this attack. Alternatively, they could steal genuine ballots beforehand. With fraudulent ballots in hand, to "stuff the ballot box," a malicious individual would have to load the ballots into the DS450 without any other election worker, partisan election judge, or public observers noticing. Even if they were able to load the ballots into the tabulator, the attacker would have to know how many absentee ballots were issued for the precinct that corresponds to the fraudulent ballots. If the tabulated total exceeds the number of absentee ballots issued, the results would be investigated. While collusion among individuals of the "Absentee Ballot Counting Board" will always be plausible, the number of individuals required to accomplish this exploit would make it highly improbable that their actions would go undiscovered.

6.1.4 EQUIPMENT TAMPERING (TABULATION MACHINE)

OVERALL RISK: LOW

Perceived Threat:	Individuals could act or a group of individuals could collude to compromise the outcome of the election by tampering with the tally in the tabulators.	
Description:	Individuals or a group of individuals could tamper with or replace the software that operates the digital tabulation machines. This could cause the machine to incorrectly tabulate votes.	
Impact:	HIGH	Changing the outcome of an election by compromising the digital tabulator's ability to accurately record votes would invalidate the results of that election. This vulnerability would be expected to have a severe impact on the integrity of the election outcome. Should the fraud be discovered, the County Auditor and the SoS would likely have to recount the ballots from the compromised tabulators by hand. This could increase costs, delay election results, and impact voter confidence.
Likelihood:	VERY LOW	Because the machines are publicly tested and verified before every election, the attacker would have a limited opportunity to compromise the tabulator without detection. When the tabulators are operating with the USB drive installed, the panels that enable access to the ports, ballot bins, and internal machine workings are locked. An attacker would have to have access to the keys, which are controlled by the County Auditor. Even if they were able to tamper with the tabulator tally, the ballot, as the single source of truth, would still reflect voters' intentions.

6.1.5 EQUIPMENT TAMPERING (USB DRIVE)

OVERALL RISK: LOW

Perceived Threat:	An individual could compromise the USB drive between the polling place and the County Auditor's office to influence election results.	
Description:	An individual could either replace or modify the USB drive at any point between its removal from the digital tabulator and its delivery to the County Auditor's office.	
Impact:	HIGH	Changing the outcome of an election by compromising the USB drive would invalidate the results of that election. This vulnerability would be expected to have a severe impact on the integrity of the election outcome. Should the fraud be discovered, the County Auditor and the SoS would likely have to recount the ballots from the compromised tabulators by hand. This could increase costs, delay election results, and impact voter confidence.
Likelihood:	VERY LOW	An attacker would have to know the manufacturer and model of the USB drive used by the vendor, source identical media, and find the opportunity to make a swap or somehow modify the drive's data in transit without detection. Even if they were able to tamper with the tabulator tally on the USB drive, the attacker would have to know how many voters had checked into the precincts or absentee ballots had been processed. If the tabulated total does not match the number of check ins on the PollPad, the results would be investigated

6.1.6 ABSENTEE BALLOT FRAUD

OVERALL RISK: LOW

Perceived Threat:	By illegitimately obtaining multiple absentee ballots, an individual could impact the outcome of an election	
Description:	Individuals could cast multiple absentee ballots and affect the outcome of an election by stealing ballots from mailboxes or friends and family, filling them out, and returning them.	
Impact:	HIGH	By casting enough fraudulent absentee ballots to change the outcome of an election, the result of that election would not be valid. Any measure passed or candidate elected would have been done so illegally. This vulnerability would be expected to have a severe impact on the integrity of the election outcome. Should the fraud be discovered, it could also impact voter confidence.
Likelihood:	VERY LOW	Voters only receive an absentee ballot if they apply for one. To prevent fraudulent applications, the information on the application must match what is in the CVF record for a voter. If the information does not match, the application is rejected. An individual would have to steal legitimately requested ballots without the victim reporting their ballot missing. Otherwise, they would have to steal a voter's identity, fraudulently request a ballot, and intercept the ballot at the victim's address before the victim sees it. In order to be counted, the signature on the back of the ballot return envelope is compared to the signature on the absentee ballot application. If the signatures do not match, the voter must verify the signature with the same form of valid ID used in the application. Unverified ballots are not included in the final tally An attacker would have to forge a voter's signature well enough to pass muster or steal a voter's identity to verify a mismatched signature. Even if the individual were able to obtain, return, and verify fraudulent absentee ballots, it is unlikely this fraud would change the outcome of an election.