

A Performance Audit of

Election Cybersecurity

Continuous Improvement to
Strengthen Security

Office of the Legislative
Auditor General

Report to the UTAH LEGISLATURE



LEGISLATIVE AUDITOR GENERAL



1975 - 2025



THE MISSION OF THE LEGISLATIVE AUDITOR GENERAL IS TO

AUDIT · LEAD · ACHIEVE

WE HELP ORGANIZATIONS IMPROVE.

Audit Subcommittee

President J. Stuart Adams, Co-Chair
President of the Senate

Senator Kirk Cullimore
Senate Majority Leader

Senator Luz Escamilla
Senate Minority Leader

Speaker Mike Schultz, Co-Chair
Speaker of the House

Representative Jefferson Moss
House Majority Leader

Representative Angela Romero
House Minority Leader

Audit Staff

Kade R. Minchey, Auditor General, CIA,
CFE

Jesse Martinson, Manager, CIA

Jake Dinsdale, Senior Audit Supervisor,
CIA

Clint Yingling, Audit Staff

Office of the Legislative Auditor General

olag.utah.gov





Office of the Legislative Auditor General

Kade R. Minchey, Legislative Auditor General

W315 House Building State Capitol Complex | Salt Lake City, UT 84114 | Phone: 801.538.1033

Audit Subcommittee of the Legislative Management Committee

President J. Stuart Adams, Co-Chair | Speaker Mike Schultz, Co-Chair

Senator Kirk Cullimore | Representative Jefferson Moss

Senator Luz Escamilla | Representative Angela Romero

April 15, 2025

TO: THE UTAH STATE LEGISLATURE

Transmitted herewith is our report:

“A Performance Audit of Election Cybersecurity” [Report #2025-08].

An audit summary is found at the front of the report. The scope and objectives of the audit are included in the audit summary. In addition, each chapter has a corresponding chapter summary found at its beginning.

[Utah Code 36-12-15.3\(2\)](#) requires the Office of the Legislative Auditor General to designate an audited entity’s chief officer. Each of Utah’s county election officials act as the chief officer over election operations in their respective locations. Due to the sensitive nature of this report and the broad scope of the audit’s findings and recommendations, the county election officials have responded to the audit collectively. As necessary and at the appropriate time, each election official is responsible for complying with our follow-up process, as well as the reporting requirements as outlined in this section of *Utah Code*.

We will be happy to meet with appropriate legislative committees, individual legislators, and other state officials to discuss any item contained in the report in order to facilitate the implementation of the recommendations.

Sincerely,

Kade R. Minchey, CIA, CFE

Auditor General

kminchey@le.utah.gov



Table of Contents

Introduction	1
Chapter 1 Stricter Internet Controls on Voting Equipment Can Enhance Cybersecurity	7
1.1 As Required by Statute, the Systems We Tested Were Not Connected to the Internet.....	7
1.2 Wireless Networking Capabilities Found in Voting Equipment Can Increase Cybersecurity Risk.....	9
Chapter 2 Election Software Is Properly Vetted; Better Controls on User Access Privileges Could Improve Security	15
2.1 Election Officials Should Better Control What Election Workers Can Access to Strengthen Cybersecurity.....	15
2.2 Election Software Is Appropriately Certified and Validated.....	17
Chapter 3 Improving Access Controls Is Needed To Strengthen Election Cybersecurity	21
3.1 Election Officials Should Strengthen Passwords to More Effectively Control User Access	21
3.2 We Found Two Instances in Which Election Computers Were Not Properly Secured.....	25
Complete List of Audit Recommendations	27
Agency Response Plan	31





PERFORMANCE AUDIT

AUDIT REQUEST

In 2023, the Legislature passed House Bill 269, which requires the Office of the Legislative Auditor General to audit the state's election system and controls every two years.

This report reflects the completion of our 2024 election audit work. The results of our efforts are also captured in *A Performance Audit of Utah's Election System (2024-20)* and *A Performance Audit of Piute and Wayne County Election Processes (2025-04)*, which we previously released.

BACKGROUND

Because election officials use computers and software products to manage elections and count ballots, cybersecurity in elections is critically important to protect the integrity of the process.

We contracted with cybersecurity experts to assess Utah's voting equipment against both legal requirements and best practices.

ELECTION CYBERSECURITY



AUDIT FINDINGS

- ✓ 1.1 – As required by statute, the systems we tested were not connected to the internet
- ✓ 1.2 – Wireless networking capabilities found in voting equipment can increase cybersecurity risk
- ✓ 2.1 – Election officials should better control what election workers can access to strengthen cybersecurity
- ✓ 2.2 – Election software is appropriately certified and validated
- ✓ 3.1 – Election officials should strengthen passwords to more effectively control user access
- ✓ 3.2 – We found two instances in which election computers were not properly secured



RECOMMENDATIONS

- ✓ The Legislature should consider prohibiting wireless communication capabilities in certain voting equipment.
- ✓ Election officials should assess users' voting equipment account privileges and ensure that all account privileges are limited to only what is strictly necessary for each user to accomplish his or her assigned duties.
- ✓ Election officials should ensure that user credentials and passwords are managed and secure.
- ✓ Election officials should create and enforce a policy requiring secure, unique passwords for each user that is granted access to voting equipment.
- ✓ As required in statute, election officials should develop and implement procedures to protect the physical security of voting equipment.

 REPORT
SUMMARY***Wireless Networking Capabilities Found in Voting Equipment Can Increase Cybersecurity Risk***

During our equipment tests, we found that the election server in one county was built using an off-the-shelf laptop—a common practice—and therefore had wireless internet components installed. Although the computer system was properly configured to prohibit internet connection, our team of experts was still able to identify significant cybersecurity concerns.

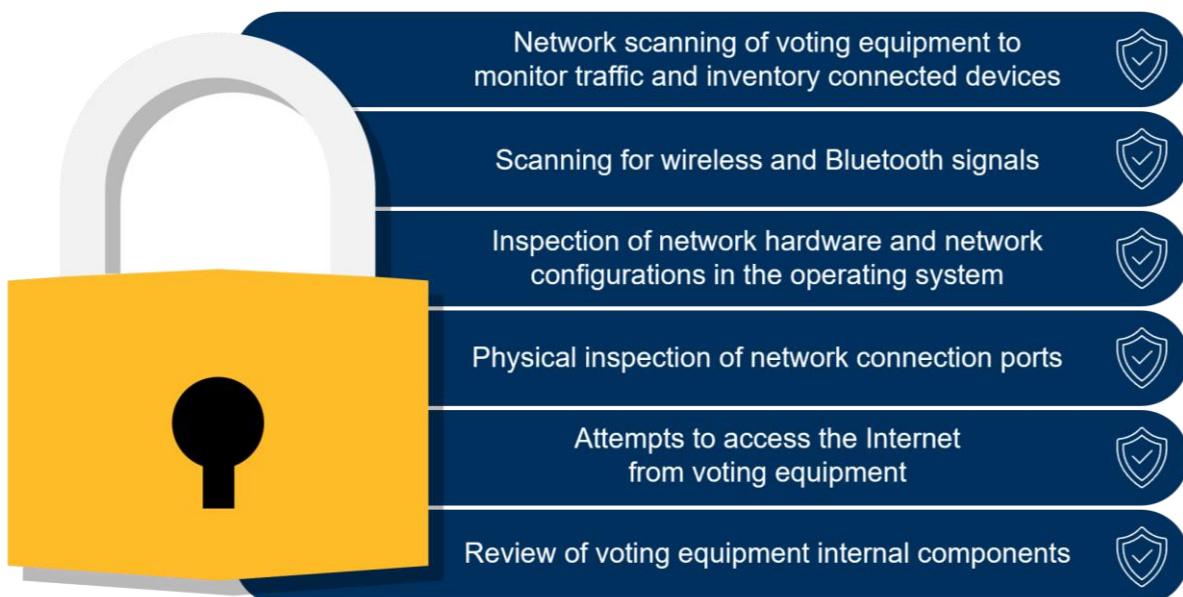
Cybersecurity best practices state that removing these wireless network components entirely would reduce the risk of misconfiguration, accidental connections, and over-the-air attacks from malicious actors.

Election Officials Should Better Control What Election Workers Can Access to Strengthen Cybersecurity

Controlling election workers' accounts and access privileges is a fundamental control for strong cybersecurity. We found that some user accounts had been granted access rights to system settings and configuration options that were not necessary to accomplish their duties.

In worst case scenarios, a malicious user could use such elevated privileges to make significant modifications to voting systems, though there are additional controls like system logs and security cameras that could help prevent and correct such an attack. While we found no evidence that these user privileges have been abused, this substantial security risk still exists.

We contracted with a team of cybersecurity experts from the Utah Education and Telehealth Network to evaluate voting equipment in a handful of Utah counties to ensure that voting equipment is not connected to the internet. Our tests found that, as required, voting equipment is not connected to the internet and that safeguards are built into systems to help prevent any unauthorized connections from happening. To come to this conclusion, our team performed multiple tests as shown here.











Introduction

To maintain the integrity of the entire voting process, election officials must follow procedures to ensure the security of election technology. Utah elections use several technological devices and systems, including our statewide voter registration system, e-poll books for in-person voting, and devices used by voters to cast ballots. This audit focuses on the equipment and systems Utah uses to scan ballots, count votes, and display election results. Statute refers to these elements as “voting equipment” and we will do the same throughout this report.

Utah Code allows the use of voting equipment as long as election officials follow the security and validation steps shown here.

 <p>Software Security Testing & Certification <i>Utah Code</i> 20A-5-802</p>	 <p>Routine Election Software Validation <i>Admin. Rule</i> R623-7-4</p>
 <p>Public Logic & Accuracy Testing <i>Utah Code</i> 20A-4-104</p>	 <p>Physical Security Controls and Logs <i>Utah Code</i> 20A-5-802 & 902</p>
 <p>No Internet Connection for Voting Equipment <i>Utah Code</i> 20A-5-903</p>	 <p>Public Post-Election Audits <i>Utah Code</i> 20A-4-104</p>

For this audit, we tested whether Utah’s voting equipment is in compliance with statute.¹ We also evaluated the equipment based on other relevant cyber security best practices. These best practices include things like data encryption, multi-factor authentication, audit logging, and ensuring that only necessary software is installed on election computers.

The US Election Assistance Commission Sets Guidelines for Election System Certification; Some States Go Further

Congress established the U.S. Election Assistance Commission (EAC) when it passed the Help America Vote Act (HAVA) in 2002. The EAC is a bipartisan commission responsible for, among other things, adopting voluntary voting

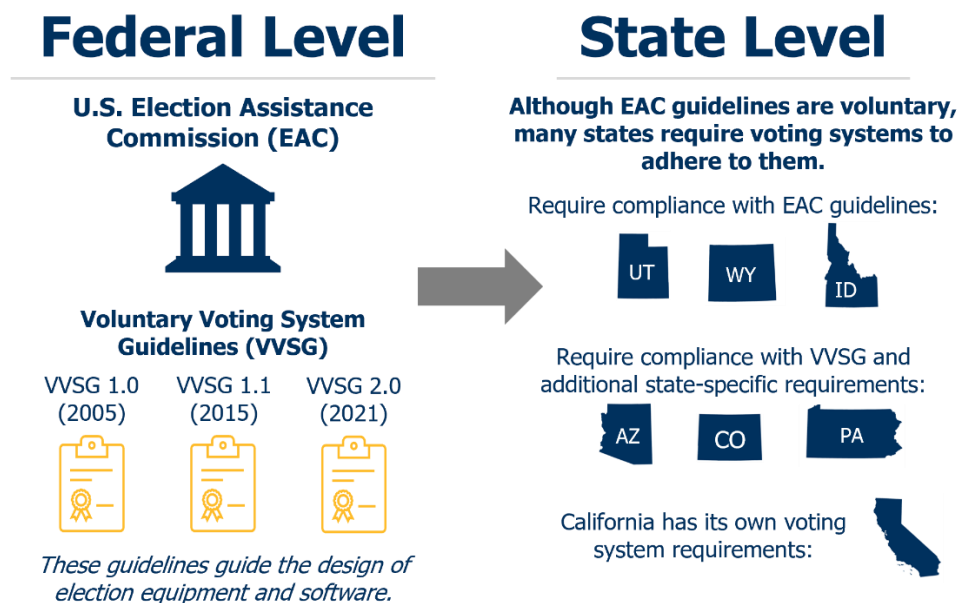
¹ In 2024, our audit team evaluated the post-election audit process and reported opportunities for improvement in *A Performance Audit of Utah’s Election System* (Report 2024-20). Given the timeline of our audit work in 2024-2025, we were unable to do a full review of logic and accuracy testing.



system guidelines, certifying voting systems, and accrediting election system testing laboratories.

As the name suggests, following the EAC’s Voluntary Voting System Guidelines (VVSG) is not required at the federal level. Nevertheless, most states—including Utah—require voting equipment to be certified to the VVSG standards as a condition of operating within the borders of the state.²

As shown here, Utah is among several other states that require VVSG certification. Some other states go beyond the VVSG, requiring voting equipment to comply with additional, state-specific requirements. California has gone even further, creating its own certification and testing requirements.



Source: Auditor generated based on federal and state voting system guidelines.

Utah’s statutory security requirements for voting equipment are considered in greater detail in the chapters of this report as we describe our findings and recommendations.

² Technically, *Utah Code* 20A-5-802 requires the Office of the Lieutenant Governor (LG’s Office) to ensure that all voting equipment is independently tested using generally accepted security testing protocols. The law then allows for the use of the EAC certification process and/or testing from an EAC accredited lab to satisfy the requirement. The LG’s Office currently exercises this option, requiring EAC certification for all voting equipment in Utah.



Our Team Contracted with Cybersecurity Experts to Test Voting Equipment in a Sample of Five Counties

To ensure that our team had the appropriate cybersecurity expertise available, we contracted with experts at the Utah Education and Telehealth Network. Their team accompanied us to the counties we selected for testing, performed security testing protocols, and helped to interpret the results.

Each county decides for itself which election equipment vendor they will use. There are currently three election equipment vendors operating in Utah's 29 counties as shown here.

Utah's Election Equipment Vendors

Dominion Voting Systems

Unisyn Voting Solutions, Inc.

Election Systems & Software (ES&S)

All testing was done on site on the actual equipment used in Utah elections. In



Some details are withheld in this report due to the sensitive nature of reporting cybersecurity threats and weaknesses.

one case, the vendor provided a cloned election laptop for primary testing and our team then corroborated our results on actual county election equipment.

Some details are withheld in this report due to the sensitive nature of reporting cybersecurity threats and weaknesses.





BACKGROUND

The primary concerns about the cybersecurity of Utah's elections focus on the potential for bad actors to compromise voting systems and manipulate election outcomes. In this chapter, we examine Utah's prohibition on internet connections for certain voting equipment. We conducted a series of tests designed to assess compliance with this requirement and relevant cybersecurity best practices.

FINDING 1.1

As Required by Statute, the Systems We Tested Were Not Connected to the Internet

No recommendation

FINDING 1.2

Wireless Networking Capabilities Found in Voting Equipment Can Increase Cybersecurity Risk

RECOMMENDATION 1.1

The Legislature should consider prohibiting wireless communication capabilities in the voting equipment listed in Utah Code 20A-5-903(1).



CONCLUSION

Our audit testing found no systems that were connected to the Internet, which complies with statute and provides significant protection against online attack from malicious actors. However, as discussed in all chapters of this report, other forms of cyber-attacks are possible and need to be protected against. Prohibiting wireless networking capabilities in voting equipment would bring Utah in line with additional best practices in this area.





Chapter 1

Stricter Internet Controls on Voting Equipment Can Enhance Cybersecurity

Utah Code prohibits election officials from connecting any equipment used for ballot marking, scanning, and tabulation to the internet.³ From a cybersecurity standpoint, a device that is never connected to the internet is protected from online attack. This practice is therefore a critical safeguard of Utah’s election integrity. However, the bulk of this report concludes that other forms of cyber-attacks are possible and need to be protected against. Several other states, including all western states surrounding Utah, have similar prohibitions on voting equipment connecting to the internet.

It is also worth noting here that controls for physical security (e.g., secure storage areas and camera surveillance) and controls for software access (e.g., account passwords, system logging, and multi-factor authentication) further reduce the risk of unauthorized access and internet connection. We discuss these elements later in the report.

1.1 As Required by Statute, the Systems We Tested Were Not Connected to the Internet

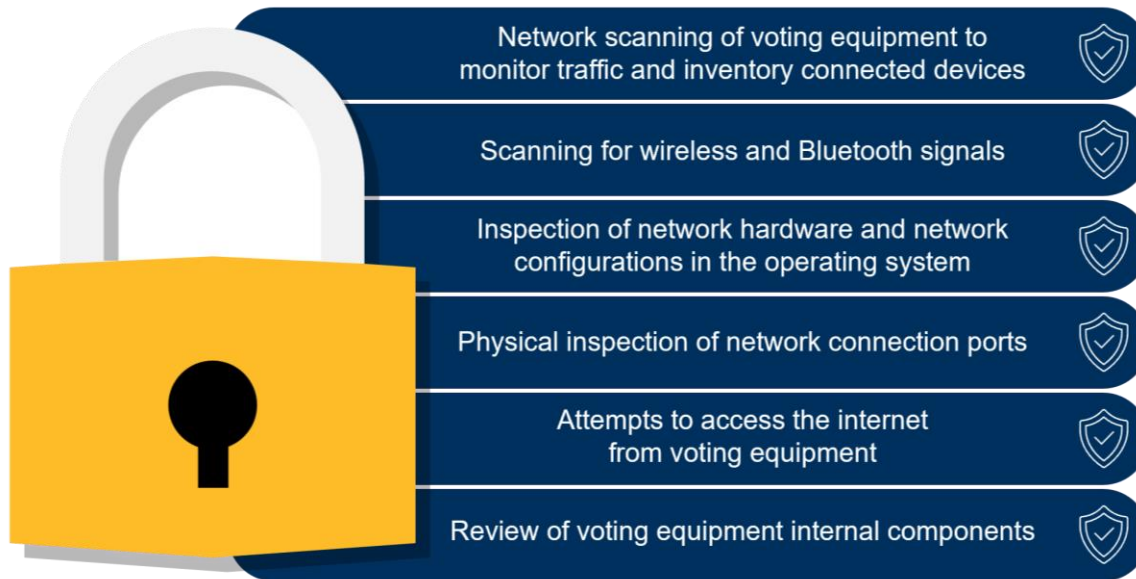


Our testing found that, as required, voting equipment is not connected to the internet.

We contracted with a team of cybersecurity experts from the Utah Education and Telehealth Network to evaluate voting equipment in a handful of Utah counties to ensure that voting equipment is not connected to the internet. Our tests found that, as required, voting equipment is not connected to the

internet and that safeguards are built into systems to help prevent any unauthorized connections from happening. To come to this conclusion, our team performed multiple tests as shown here.

³ *Utah Code* 20A-5-903



Source: Auditor generated

Voting Equipment Is Configured to Help Minimize the Risk of Unauthorized Network Connections

In addition to confirming that voting equipment is not connected to the internet through either wired or wireless means, we also found protections that are built into election software and operating systems to limit internet connections. For example, we found instances where operating systems were intentionally configured so a user couldn't see or access network devices within the operating system.

On another piece of equipment, the system was configured to limit connections to anything outside a local network, which some counties use to connect multiple pieces of election equipment. Two of our test counties established such local networks to link voting equipment together to aid in ballot scanning and adjudication. Our tests found that these local networks were not connected to the internet and that no unauthorized devices were present.

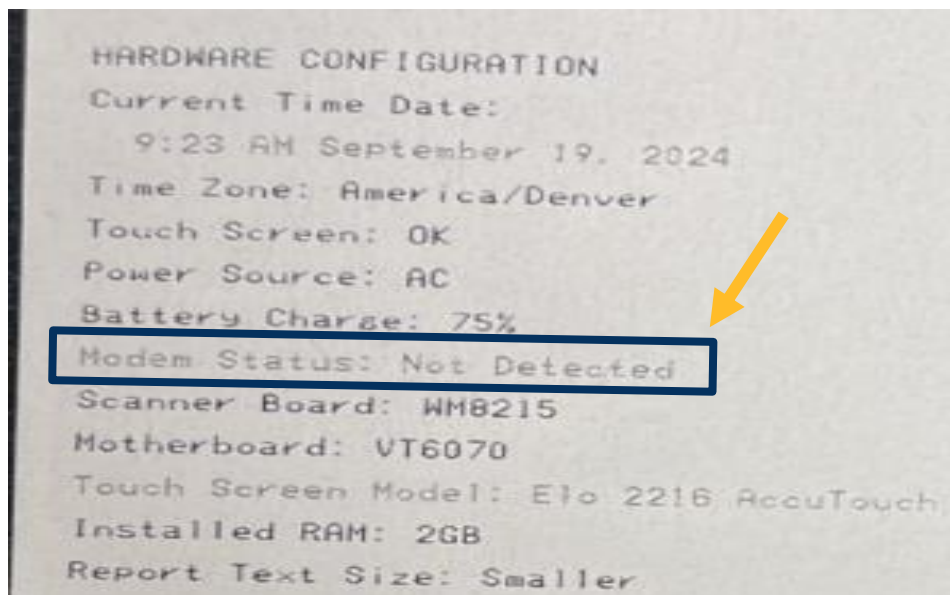


Protections are built into voting equipment and software to prevent internet connections.

As we physically inspected the hardware within certain pieces of election equipment, we confirmed that there were no network cards or modems. Without these items, the equipment cannot connect to the internet or to a local network. We then observed that configuration reports regularly printed from these machines—a portion of which is shown below—provide a confirmation of this lack of networking equipment, providing transparency and an audit trail.



Figure 1.1 This Configuration Report Confirmed That a Modem Was Not Present in A Ballot Scanner We Inspected. These printed reports can serve as an audit trail for proper voting equipment configuration.



Source: Auditor photo taken during inspection of voting equipment.

1.2 Wireless Networking Capabilities Found in Voting Equipment Can Increase Cybersecurity Risk

During our equipment tests, we found that the election server in one county was built using an off-the-shelf laptop—a common practice—and therefore had wireless internet components installed. Although the computer system was properly configured to prohibit internet connection, our team of experts was still able to identify significant cybersecurity concerns.⁴



Removing wireless networking hardware can prevent misconfiguration and accidental connections.

Cybersecurity best practices state that removing these wireless network components entirely would reduce the risk of misconfiguration, accidental connections, and over-the-air attacks from malicious actors. The election vendor for the county explained that similar laptop-based servers they have deployed in recent years have had their wireless components removed entirely.

⁴ This report does not identify the specific concerns as a security measure.



The National Institute of Standards and Technology notes that, “many computers that host the [Election Management System]⁵ are laptops which have wireless internet capacity installed which could make them vulnerable to online attacks.” They go on to recommend that “Wireless networks (WiFi and even Bluetooth) should be avoided on networks that are supposed to be isolated.”⁶

Pursuant to statute, the Office of the Lieutenant Governor (LG’s Office) requires election equipment to be certified to U.S. Election Assistance Commission (EAC) standards. In its recently revised standards, the EAC warns against the risk of wireless connections.

Voluntary Voting System Guidelines (VVSG) 2.0:

“Wireless connections can expand the attack surface of the voting system by opening it up to over-the-air attacks. Over-the-air access can allow for adversaries to attack remotely without physical access to the voting system. By disallowing wireless capabilities in the voting system, this limits the attack surface and restricts any network connections to be hardwired.”

Although Utah is already poised to adhere to the EAC’s new guidelines prohibiting wireless connections, the guidelines stop short of requiring the full removal of wireless hardware. In our testing and discussions with Utah’s election stakeholders, we found that prohibiting wireless hardware in election equipment in Utah would reduce the risks articulated above without negatively impacting the function of our election equipment.

Some States’ Laws Prohibit Wireless Connection Capabilities in Voting Equipment

Some states specifically prohibit wireless *connections* in statute or administrative code. Utah’s statute already effectively does this.⁷ Some states go further, prohibiting even wireless connection *capabilities*. We believe that Utah could strengthen our election cyber security posture by taking the latter approach. The following table shows different approaches across multiple states.



Some states prohibit wireless connection capabilities in voting equipment.

⁵ The Election Management System, or EMS, is a term used across election equipment vendors to describe the core software each system uses to tabulate results and generally manage elections.

⁶ *Voting: Security Recommendations*. U.S. Department of Commerce – National Institute of Standards and Technology. Updated February 2021.

⁷ *Utah Code* 20A-5-903



Texas	Amended statute in 2021 to read, “a voting system may not have the capability of permitting wireless communication.”	Section 129.054(b) of the Texas Election Code
Nevada	“Nevada's voting system is a ‘standalone system’ that is not connected to a network, the Internet, and does not have wireless connection capabilities.”	Nevada Secretary of State’s Election Procedures Manual – Chapter 9: Voting Systems
Ohio	“The equipment shall not connect to the internet. If submitted for testing for certification by the federal election assistance commission on or after June 16, 2021, the equipment does not contain any wireless communication hardware or software components.”	Ohio Admin. Code – Rule 111:3-9-08(B)(3)
California	“These standards prohibit wireless communications capabilities in voting systems.”	California Voting System Standards – 7.1.2

In addition to the existing prohibition on connecting voting equipment to the internet, we believe that the Legislature should consider amending statute to reduce the risk of wireless network vulnerabilities by specifically prohibiting wireless communication capabilities in voting equipment. Our testing of election equipment during this audit supports the value of this recommendation.

RECOMMENDATION 1.1

The Legislature should consider prohibiting wireless communication capabilities in the voting equipment listed in *Utah Code* 20A-5-903(1).





BACKGROUND

In our review of voting-equipment security, we evaluated whether the software was properly vetted and certified before it was installed for use in Utah elections. We also evaluated election equipment and software systems against cybersecurity best practices.

FINDING 2.1

Election Officials Should Better Control What Election Workers Can Access to Strengthen Cybersecurity

RECOMMENDATION 2.1

Election officials, working with election vendors as necessary, should create an inventory of all user accounts granted to individuals on voting equipment and assess whether access privileges are appropriately matched to each user's legitimate system needs.

RECOMMENDATION 2.2

Election officials should ensure that all users' account privileges (as inventoried under Recommendation 2.1) are limited to only what is strictly necessary for each user to accomplish his or her assigned duties.

FINDING 2.2

Election Software Is Appropriately Certified and Validated

No recommendation



CONCLUSION

Our testing found that election software and hardware consisted of legitimate, vetted, and certified versions as required in *Utah Code*. Further, our evaluation team found multiple layers of cybersecurity practices that help ensure that only valid election software is used in Utah elections. That said, we also found opportunities for counties and vendors to work together to better control user access privileges within the software.





Chapter 2

Election Software Is Properly Vetted; Better Controls on User Access Privileges Could Improve Security

In our review of voting-equipment security, we evaluated whether the software was properly vetted and certified before it was installed for use in Utah elections. We also evaluated election equipment and software systems against cybersecurity best practices. Our testing found that installed software and hardware consisted of legitimate, vetted, and certified versions as required in *Utah Code*. Further, our evaluation team found multiple layers of cybersecurity practices that help ensure that only valid election software is used in Utah elections. That said, we also found opportunities for counties and vendors to work together to better control user access privileges within the software. Tightening this access would reduce the state’s exposure to potential nefarious actions and improve election cybersecurity.

It is important to note that that in our testing, our team of experts identified multiple layers of cybersecurity controls that serve to mitigate some of the risk we describe in this chapter. Malicious actors would need to gain access to controlled areas, user credentials, and, in some cases, multi-factor authentication credentials before they can even attempt the attacks discussed in this chapter. That said, the risk of insider attack is a valid concern as we consider ways to strengthen our security practices.

2.1 Election Officials Should Better Control What Election Workers Can Access to Strengthen Cybersecurity



Controlling election workers’ accounts and access privileges is a fundamental control for strong cybersecurity. We found that some user accounts had been granted access rights to system settings and configuration options that were not necessary to accomplish their duties. Granting users unnecessary administrative access like this can enable them to make changes to parts of a computer system without restrictions, increasing the risk of misuse or attack. In worst case scenarios, a malicious actor could use such elevated privileges to make significant modifications to voting systems, though there are additional controls like system logs and security cameras that could help prevent and



correct such an attack. While we found no evidence that these user privileges have been abused, this substantial security risk still exists. Election officials should better control administrative access to ensure that authorized users can only use software in ways that are directly related to their duties.

According to the National Institute of Standards and Technology, the principle of least privilege states that, “a system should restrict the access privileges of users...to the minimum necessary to accomplish assigned tasks.” By following this principle, systems and access rights can be structured to limit users from accessing system settings and configurations that could be used in unauthorized and inappropriate ways.

An FBI report about insider threats to elections describes a case in which a temporary election worker inserted an unauthorized personal flash drive into election equipment and stole confidential voter data.⁸ The report goes on to state that limiting this user’s access within the system could have been one way to prevent the data theft.

Although we found no evidence that any unauthorized election system changes or access have taken place, we believe that the potential for misuse of access is serious enough to act. Counties and vendors across the state should work together to review users’ access privileges and ensure that they appropriately restrict access to only what is necessary to accomplish each user’s specific election-related tasks. As a comparison, *Administrative Rule* requires a similar process of review and control for user accounts granted to the state’s voter registration system.⁹



Election officials should better control users’ administrative access to ensure that they can only use software in ways that are directly related to their duties.

RECOMMENDATION 2.1

Election officials, working with election vendors as necessary, should create an inventory of all user accounts granted to individuals on voting equipment and assess whether access privileges are appropriately matched to each user’s legitimate system needs.

⁸ See *2024 U.S. Federal Elections: The Insider Threat*, issued by the FBI in a joint effort with the Department of Homeland Security’s Office of Intelligence and Analysis, the Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Election Assistance Commission (EAC).

⁹ *Administrative Rule* R623-10-4



RECOMMENDATION 2.2

Election officials should ensure that all users’ account privileges (as inventoried under Recommendation 2.1) are limited to only what is strictly necessary for each user to accomplish his or her assigned duties.

2.2 Election Software Is Appropriately Certified and Validated

Before voting equipment can be used in Utah, it goes through three main steps to ensure its security. Voting equipment is

- Certified to federal voting system standards
- Certified by the Utah Office of the Lieutenant Governor
- Installed on equipment deployed in the counties

Our review found that the voting software and systems in use in Utah have been appropriately certified and approved according to the process described in statute.¹⁰

To confirm that the software versions installed were identical to what has been certified and approved, we examined the processes used to deploy equipment and software systems across the state. Election vendors use encryption and validation techniques to ensure that the software that is installed on Utah’s voting equipment is a version that has been properly certified.

Hash Validation Provides Digital Confirmation that Election Software Has Not Been Manipulated

To independently corroborate the strength of these processes, we observed hash validations for county election software. Our observations confirmed that the



Hash validation is a technique used in Utah to ensure that election software is unchanged from its authorized version.

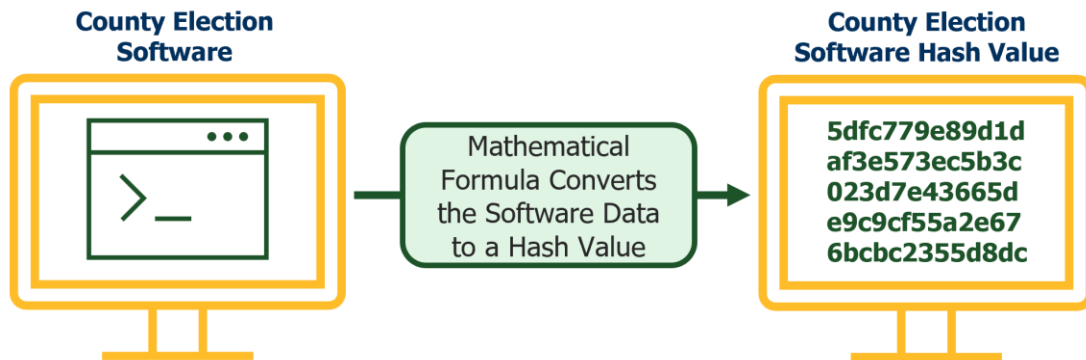
voting equipment software used by the counties was the authorized, unchanged version of the software.

In a hash validation, an independent, preferably open-source software tool uses a commonly known formula to convert a computer program into a series of numbers and letters known as a hash value. Anyone in the world who uses the same formula to convert the same computer program will get the same

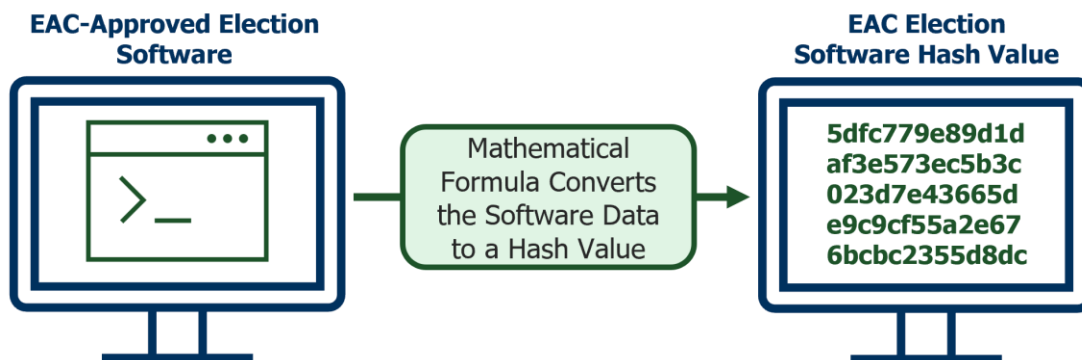
¹⁰ *Utah Code* 20A-5-802



hash value. More importantly, if the computer program is manipulated in any way, the hash value will change.



Once a county calculates the hash value for their software, they then request the hash value for the same software from a trusted source like the U.S. Election Assistance Commission (EAC). The EAC runs the same mathematical formula on what they know is the authorized version of the election software—because they are the ones that authorized it—and they provide that hash value to the county.



If the hash value the county calculated matches the hash value provided by the trusted source, the user can know that their software is the correct, unmanipulated version that is safe for use.

In three instances, we were physically present during the hash validation procedures. *Administrative Rule* requires election officials to perform their own regular hash validations of voting equipment software to independently confirm that the appropriate versions have been installed and to help ensure that system files have not been tampered with.¹¹

¹¹ *Administrative Rule* R623-7



BACKGROUND

Because voting equipment in Utah is not connected to the internet, protecting physical access is important to safeguard against a cyber-attack. Therefore, things like physical access controls (e.g., locks on doors, secure equipment storage, etc.) and user access controls (e.g., user passwords, multi-factor authentication) are critical for election cybersecurity.

FINDING 3.1 **Election Officials Should Strengthen Passwords to More Effectively Control User Access**

RECOMMENDATION 3.1

Election officials should make use of a password administrator as directed by the Utah Elections Handbook or otherwise ensure that user credentials and passwords are managed and secure.

RECOMMENDATION 3.2

Election officials should consult with guidelines from credible cybersecurity organizations, like those provided here, to create and enforce a policy requiring secure, unique passwords for each user that is granted access to voting equipment.

FINDING 3.2 **We Found Two Instances in Which Election Computers Were Not Properly Secured**

RECOMMENDATION 3.3

As required in statute, the election officials in the affected counties should develop and implement procedures to protect the physical security of voting equipment.



CONCLUSION

In our testing and observations, our main concerns with access controls were:

- Opportunities for election officials to improve the management and strength of user passwords
- Two instances in which counties did not store voting equipment in secure locations, which runs contrary to statutory requirements for physical security

Because Utah has multiple layers of controls that work together to help prevent cyber-attack, ensuring that all control layers are optimized will help prevent someone from disrupting or undermining elections.





Chapter 3

Improving Access Controls Is Needed to Strengthen Election Cybersecurity

Because voting equipment in Utah is not connected to the internet, protecting physical access is important to safeguard against a cyber-attack. Therefore, things like physical access controls (e.g., locks on doors, secure equipment storage, etc.) and user access controls (e.g., user passwords, multi-factor authentication) are critical for election cybersecurity. Implementing robust access controls can help prevent attacks like someone inserting an unauthorized USB drive, an election worker gaining unauthorized access to programs or files, or someone simply vandalizing voting equipment with the intent to disrupt the process.

In our testing and observations, our main concerns with access controls were

- Opportunities for election officials to improve the management and strength of user passwords
- Two instances in which counties did not store voting equipment in secure locations, which runs contrary to statutory requirements for physical security

Because Utah has multiple layers of controls that work together to help prevent cyber-attack, ensuring that all control layers are optimized will help prevent someone from disrupting or undermining elections.

3.1 Election Officials Should Strengthen Passwords to More Effectively Control User Access

The security of voting systems relies heavily on denying access to unauthorized users. When used correctly, strong passwords can help protect against such unauthorized access. Our audit found multiple opportunities for election officials to strengthen this user authentication control—like storing passwords securely and creating stronger, unique passwords—to help ensure that only authorized personnel have access Utah’s critical election systems.



There are opportunities for election officials to strengthen passwords to protect critical election systems.



Some Election-Related User Passwords Were Not Stored Securely, Increasing the Risk of Unauthorized Access to Election Systems

Our election cybersecurity tests found that some users stored passwords on paper notes, undermining the security that good password management can provide. For example, during the November 2024 election, we visited one county and found that users had created a reference card with username and password information for multiple systems and were keeping the card next to a computer used for elections. The county clerk was unaware that staff were doing this.

Figure 3.1 Election Login Credentials Were Not Adequately Protected. Doing this creates an obvious risk for unauthorized access to critical election systems.



Source: Auditor photo taken during the November 2024 General Election.

In addition to those in the photograph in Figure 3.1, we found other counties storing passwords on paper during our assessment. Storing passwords in this way could allow someone to much more easily gain unauthorized access to vital election tools like the voter registration database or the state election results website, which could lead to data manipulation or other efforts to undermine the election process.



Despite compensating controls, storing passwords on paper near election workstations weakens election cybersecurity.

Although this is clearly not a safe way to manage passwords, the county was also employing compensating controls. We also observed efforts to control access to the room where the computer was located and at least one layer of multi-factor authentication is in place that could disrupt unauthorized login attempts on certain portions of election-related systems. Nevertheless, election officials must manage passwords better to create as

many barriers to attack as possible.

Additionally, we found a password that was stored in a plain text file alongside its corresponding digital certificate on a user's computer desktop. While we did



not confirm the purpose of the certificate or whether it was in use, storage of a password in plain text in the same location as the certificate is a noteworthy security weakness.

Protecting Passwords Can Prevent a Malicious User from Getting a Foot in the Door. According to cybersecurity experts, human errors—like leaving passwords out in the open—can be one of the biggest cyber vulnerabilities and therefore must be managed. Once bad actors gain access to a system with legitimate credentials, they can steal sensitive data, infect systems with malware, move more covertly through systems and networks, and expand their attack by obtaining more and more access.



Users' passwords must be well managed to prevent potentially damaging attacks.

To better protect against unauthorized access, the Utah Elections Handbook, provided by the LG's Office, states that someone in each election office should be designated as a password administrator.

Utah Election Handbook – 14.D

"The password administrator's duties are as follows:

- (1) create unique passwords for each election;*
- (2) maintain a master list of all passwords created in a secure location;*
- (3) recreate passwords periodically; and*
- (4) monitor password usage.*

Utah's election officials should work to eliminate password-related vulnerabilities like the ones detailed here and ensure that user credentials for critical election systems, including passwords, are managed and secure.

RECOMMENDATION 3.1

Election officials should make use of a password administrator as directed by the Utah Elections Handbook or otherwise ensure that user credentials and passwords are managed and secure.

Some Passwords Were Reused or Lacked Adequate Complexity

The National Institute of Standards and Technology states that strong passwords should be "of sufficient complexity and secrecy that it would be impractical for an attacker to



We found a handful of instances in which users weren't following best practices for password creation.

guess or otherwise discover the correct secret value.”¹² In our review, we found a handful of instances in which users weren't following best practices for password creation.

In one case, we found that account passwords were being reused across similar election devices. This could allow a user to gain access to a device other than the one he or she is authorized to use. We also observed one county that used a similar prefix across multiple passwords such that each password was a variation on that “base” prefix. If a malicious actor determines that all passwords share a common word or phrase, this can increase the likelihood that password can be compromised. Additionally, our testing of county computers used to access state-level election systems found that users' password complexity and strength did not meet current standards.

It is important to note that the vulnerabilities created by these password deficiencies are mitigated through physical access controls and, in some cases, additional layers of authentication. Nevertheless, we believe that election officials should ensure that the passwords used to authenticate users on election and election-related systems follow best practices to help prevent unauthorized access to these critical systems.

While best practices from different cybersecurity organizations may differ in their specific recommendations, they all agree that passwords should be sufficiently long, complex, and unique to reasonably prevent an unauthorized user from discovering the secret value. Election officials should therefore work with their equipment vendors and consult guidelines like those from NIST, the U.S. Election Assistance Commission, and/or the Center for Internet Security as a guide to create secure, unique passwords for each user who is granted access to voting equipment.¹³



Election officials should work to create secure, unique passwords for each user who is granted access to voting equipment.

¹² *Special Publication 800-63B: Digital Identity Guidelines*. National Institute of Standards and Technology (NIST). June 2017; updated March 2020.

¹³ Useful publications from these entities include *Special Publication 800-63B: Digital Identity Guidelines*, NIST; *Election Management Guidelines - Chapter 6: System Security*, U.S. Election Assistance Commission; and the *CIS Password Policy Guide*, Center for Internet Security.



RECOMMENDATION 3.2

Election officials should consult with guidelines from credible cybersecurity organizations, like those provided here, to create and enforce a policy requiring secure, unique passwords for each user that is granted access to voting equipment.

3.2 We Found Two Instances in Which Election Computers Were Not Properly Secured

Because Utah’s voting equipment is prohibited from connecting to the internet, a malicious actor would need physical access to controlled areas, computers, tabulation machines, USB sticks, etc. to carry out an attack. Physical security controls are therefore an important part of guarding election integrity. Not only do well executed physical security controls protect against outside threats, but they can help prevent insider threats as well.

We observed two instances in which voting equipment was not properly secured. Specifically, we found that the main election computers in two counties were in unsecured locations to which members of the public had regular access. Limiting physical access to these critical computer systems is a key election control as shown in the statute referenced here.

Utah Code 20A-5-802(1)(b)

For the voting equipment used in the jurisdiction over which an election officer has authority, the election officer shall...develop and implement a procedure to protect the physical security of the voting equipment;

In addition to statute, the Utah Elections Handbook issued by the LG’s Office states that, “components of the electronic voting system...must be stored in a locked, secured location that prevents unauthorized access.”

The clerks in these counties are aware of these concerns and are working to overcome constraints to improve the physical security of their voting equipment. Our recommendation here will help ensure that we can continue to follow up on the implementation of proper security procedures.

It is important to note that we have observed other counties across the state working to ensure that their election equipment is properly secured.



RECOMMENDATION 3.3

As required in statute, the election officials in the affected counties should develop and implement procedures to protect the physical security of voting equipment.



Complete List of Audit Recommendations



Complete List of Audit Recommendations

This report made the following six recommendations. The numbering convention assigned to each recommendation consists of its chapter followed by a period and recommendation number within that chapter.

Recommendation 1.1

We recommend that the Legislature consider prohibiting wireless communication capabilities in the voting equipment listed in Utah Code 20A-5-903(1).

Recommendation 2.1

We recommend that election officials, working with election vendors as necessary, create an inventory of all user accounts granted to individuals on voting equipment and assess whether access privileges are appropriately matched to each user's legitimate system needs.

Recommendation 2.2

We recommend that election officials ensure that all users' account privileges (as inventoried under Recommendation 2.1) are limited to only what is strictly necessary for each user to accomplish his or her assigned duties.

Recommendation 3.1

We recommend that election officials make use of a password administrator as directed by the Utah Elections Handbook or otherwise ensure that user credentials and passwords are managed and secure.

Recommendation 3.2

We recommend that election officials consult with guidelines from credible cybersecurity organizations, like those provided here, to create and enforce a policy requiring secure, unique passwords for each user that is granted access to voting equipment.

Recommendation 3.3

We recommend that election officials in the counties mentioned in Finding 3.2 develop and implement procedures to protect the physical security of voting equipment as required in statute.





Agency Response Plan





Response to the Election Cybersecurity Audit by the Legislative Auditor General

April 3, 2025

Kade R. Minchey, CIA, CFE, Auditor General
Office of the Legislative Auditor General
Utah State Capitol Complex
Rebecca Lockhart House Building, Suite W315
Salt Lake City, UT 84114-5315

Dear Mr. Minchey,

Thank you! We were excited to be selected for an Election Cybersecurity audit. The Clerks of Utah's 29 counties constantly seek to improve the security and integrity of Utah's elections, and we want to thank the auditors for their professionalism and dedication to help us in this effort.

We are pleased that the extensive and thorough audit testing has confirmed what we have been saying for years: election systems in Utah are secure and protected by, as the audit states, "multiple layers of cybersecurity practices," specifically:

- Voting systems are not connected to the Internet
- Voting equipment is properly configured to help minimize the risk of cyber-attacks
- Election software is appropriately certified and validated
- Physical security controls, user credentials, system logs, hash audits, multi-factor authentication, and security cameras provide additional security

We have included our responses to the specific recommendations in the audit on the next page.

Utah's 29 County Clerks remain steadfast in our commitment to safeguarding the integrity of our elections. We recognize that cybersecurity is an ongoing effort, and we will continue to adapt and improve to ensure our elections remain among the most secure in the nation. Voter confidence is paramount, and we are dedicated to earning and preserving that trust through full transparency, unwavering vigilance, and continuous improvement.

Sincerely,

Utah's 29 County Clerks

Recommendation 1.1: The Legislature should consider prohibiting wireless communication capabilities in the voting equipment listed in Utah Code 20A-5-903(1).

Response from County Clerks: This recommendation relates to the Legislature, not the County Clerks. However, County Clerks support the recommendation and join the auditors in recommending the Legislature establish this provision in statute.

Recommendation 2.1: Election officials, working with election vendors as necessary, should create an inventory of all user accounts granted to individuals on voting equipment and assess whether access privileges are appropriately matched to each user's legitimate system needs.

Response from County Clerks: We have already added training to our next two conference agendas (both to be held before the next election in August) to implement this recommendation. We will make these inventories available to the Legislative Auditors as part of their follow up.

Recommendation 2.2: Election officials should ensure that all users' account privileges (as inventoried under Recommendation 2.1) are limited to only what is strictly necessary for each user to accomplish his or her assigned duties.

Response from County Clerks: This recommendation will be implemented at the same time and can be verified on the same documents as Recommendation 2.1.

Recommendation 3.1: Election officials should make use of a password administrator as directed by the Utah Elections Handbook or otherwise ensure that user credentials and passwords are managed and secure.

Response from County Clerks: We have already added training to our next two conference agendas (both to be held before the next election in August) to implement this recommendation. Each county will provide the name of the password administrator to the Legislative Auditors during their follow up.

Recommendation 3.2: Election officials should consult with guidelines from credible cybersecurity organizations, like those provided here, to create and enforce a policy requiring secure, unique passwords for each user that is granted access to voting equipment.

Response from County Clerks: We have already added training to our next two conference agendas (both to be held before the next election in August) to implement this recommendation. Each county will make their password policy available to the Legislative Auditors during their follow up.

Recommendation 3.3: As required in statute, the election officials in the affected counties should develop and implement procedures to protect the physical security of voting equipment.

Response from County Clerks: The counties referred to in this section make up less than 1% of the state's population and have already implemented the recommendation. We will also discuss this recommendation at our next two conferences, which will be held before the next election in August.



THE MISSION OF THE LEGISLATIVE AUDITOR GENERAL IS TO

AUDIT · LEAD · ACHIEVE

WE HELP ORGANIZATIONS IMPROVE.
