



**A Report to the  
Audit Committee**

**Mayor**  
John Cooper

**Administrator of Elections**  
Jeff Roberts

**Audit Committee Members**  
Kevin Crumbo  
Charles Frasier  
Thom Druffel  
Brackney Reed  
Jim Shulman  
Zulfat Suara

**Davidson County Election  
Commission Information Systems  
Audit**

September 4, 2020

Metropolitan  
Nashville  
Office of  
Internal Audit

**EXECUTIVE SUMMARY**  
September 4, 2020



**Why We Did This Audit**

The audit was conducted due to the importance of ensuring the integrity and fairness of elections conducted in Davidson County.

**What We Recommend**

- Implement processes to ensure access removal of terminated employees.
- Perform and document an annual risk assessment in accordance with *Tennessee Elections Security Standard*.
- Perform quarterly reviews of firewall rules and ensure reviews are documented.
- Establish a process to ensure employees receive security training in accordance with the *Tennessee Elections Security Standard*.
- Develop and document cybersecurity and employee acceptable use policies.

**DAVIDSON COUNTY ELECTION COMMISSION  
INFORMATION SYSTEMS AUDIT**

**BACKGROUND**

The mission of the Davidson County Election Commission is to provide free and fair local, state, and federal elections to every eligible citizen of Davidson County, so they have equal access to the election process and exercise their right to vote.

**OBJECTIVES AND SCOPE**

KraftCPAs PLLC was retained to evaluate the design and effectiveness of the internal controls related to the Election Commission for the period March 1, 2019 through February 29, 2020. Procedures were designed to assess compliance with the Tennessee Elections Security Standard. Areas of audit emphasis included, but were not limited to:

- Information security policies and procedures are in place and followed;
- A secure computing environment and network are maintained;
- Logical security controls are in place to protect systems;
- Encryption is used where appropriate to protect voter data and election systems;
- Endpoint protections are used to protect systems;
- Access to voter data is restricted and follows minimum necessary standards;
- Physical security controls are in place to protect systems;
- Vendor management procedures are appropriate to protect systems;
- Monitoring is used to track, alert, and analyze access to network resources and voter data;
- The Election Commission assesses internal systems and processes; and
- Change control has been implemented to protect systems.

**WHAT WE FOUND**

The following table identifies the functional area tested where observations exist, along with the number of observations by risk level. Red reflects audit observations that are considered high risk, yellow reflects audit observations of medium risk, and green reflects observations of low risk.

Internal Audit Area	Auditor's Grade	High	Medium	Low	Page	
Removal of Access for Terminated Employee	Needs Improvement	1	-	-	5	
Documented Risk Assessment		-	1	-	5	
Workstation Lockout Configurations		-	1	-	6	
Insufficient Review of Firewall Rules		-	1	-	6	
Encryption Key Custodian Acknowledgements		-	1	-	6	
Inconsistent Information Security Training		-	1	-	7	
Insufficient Policy Documentation		-	1	-	7	
Insufficient User Access Reviews		-	-	-	1	8
<b>Total</b>			<b>1</b>	<b>6</b>	<b>1</b>	

Chart page numbers refer to the KraftCPAs PLLC full report, Appendix A.

## **GOVERNMENT AUDITING STANDARDS COMPLIANCE**

---

We conducted this performance audit in accordance with generally accepted government auditing standards. 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 observations and conclusions based on our audit objectives.

## **METHODOLOGY**

---

To accomplish our audit objectives, we performed the following steps:

- KraftCPAs PLLC was hired to assist with this engagement.
- The detailed methodology employed by KraftCPAs PLLC can be found in **Appendix A**.

## **AUDIT TEAM**

---

### KraftCPAs PLLC

Scott Nalley CPA, CIA, CISA, Member  
Erica Hightower, CPA, CISA, Supervisor  
Mike Wilson, CPA, CISA, CISSP, Supervisor  
Bryan Malle, Senior Auditor

### Metropolitan Nashville Office of Internal Audit

Lauren Riley, CPA, CIA, ACDA, CMFO, Metropolitan Auditor

## **APPENDIX A – Report From KraftCPAs PLLC**

---

KraftCPAs PLLC was hired to assist with this engagement. The firm issued a report to the Office of Internal Audit, with details on objectives, methodology, observations, and recommendations. The report begins on the next page.

# Metropolitan Government of Nashville and Davidson County

## Election Commission Information Systems Audit Internal Audit Report

For the period  
March 1, 2019 through February 29, 2020



---

*This audit was performed at the request of the Metropolitan Nashville Office of Internal Audit. As such, the Tennessee Open Records Act makes this report subject to public disclosure.*

# Metropolitan Government of Nashville and Davidson County

## Election Commission Information Systems Audit

### Table of Contents

---

I. Executive Summary.....	2
II. Overview of Results .....	3
III. Observations and Conclusion Summary .....	4
IV. Observations and Recommendations.....	5

---

#### Report Distribution:

<u>Name</u>	<u>Title</u>
Jeff Roberts	Administrator of Elections
Keith Durbin	Director of Information Technology Services
John Griffey	Assistant Director, Information Technology Services

#### Additional Distribution:

<u>Name</u>	<u>Title</u>
Lauren Riley	Metropolitan Auditor

**I. Executive Summary**

**Introduction**

KraftCPAs PLLC performed certain internal audit services for The Metropolitan Government of Nashville and Davidson County Office of Internal Audit related to Election Commission information systems. Our services were performed in accordance with contract number 433868 between The Metropolitan Government of Nashville and Davidson County (Metro) and KraftCPAs PLLC. We conducted this audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide 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.

**Audit Scope and Objectives**

Our primary objective was to evaluate the design and effectiveness of the internal controls related to the Election Commission for the period March 1, 2019 through February 29, 2020. Our procedures were designed to assess compliance with the *Tennessee Elections Security Standard*. Areas of audit emphasis included, but were not limited to:

- Information security policies and procedures are in place and followed;
- A secure computing environment and network are maintained;
- Logical security controls are in place to protect systems;
- Encryption is used where appropriate to protect voter data and election systems;
- Endpoint protections are used to protect systems;
- Access to voter data is restricted and follows minimum necessary standards;
- Physical security controls are in place to protect systems;
- Vendor management procedures are appropriate to protect systems;
- Monitoring is used to track, alert, and analyze access to network resources and voter data;
- The Election Commission assesses internal systems and processes; and
- Change control has been implemented to protect systems.

In order to achieve our audit objectives, we performed the following procedures:

- Reviewed applicable laws and regulations;
- Gained an understanding of processes and controls in place during the audit period; and
- Tested controls implemented by the Election Commission to meet the *Tennessee Elections Security Standard*. Testing procedures included the following:

<b>Test</b>	<b>Description</b>
Inspection	Inspected documents and reporting indicating performance of control activity.
Observation	Observed application of specific control activities.
Inquiry	Inquired with key personnel and corroborated responses with management.

## II. Overview of Results

During the course of our work, we discussed potential observations with management. A summary of key issues is provided later in **Section III** along with our risk level assessment.

In order to enhance your understanding of each specific observation, we have provided a risk level, defined as follows:

**High** - Requires immediate management attention. This is a serious internal control or risk management issue that may, with a high degree of certainty, lead to substantial losses, serious reputation damage, or significant adverse impact.

**Medium** - Requires timely management attention. This is an internal control or risk management issue that may lead to financial losses, reputation damage, or adverse impact, such as public sanctions or immaterial fines.

**Low** - Routine management attention is warranted. This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the process being tested. Risks are limited.

Based on our procedures and assessment of the observations noted, we have provided an overall audit grade. The audit grade is not intended to usurp ultimate risk assessment responsibility, which is vested with the audit committee and management. Overall audit grades are defined as follows:

**Satisfactory** - Observations are limited to minor deviations from policy or regulatory requirements resulting in nominal risk to the organization. The design and operating effectiveness of controls evaluated during the audit appear adequate and reasonable. However, because of inherent limitations in any system of internal control, errors or irregularities may occur and not be detected. Therefore, absolute reliance should not be placed on these controls.

**Needs Improvement** - Observations include an aggregation of minor deviations and/or major deviations from policy or regulatory requirements resulting in reasonable probability of further misstatements or violations, if not corrected promptly. The design and operating effectiveness of controls evaluated during the audit appear to be less than adequate, and limited reliance can be placed on these controls.

**Unsatisfactory** - Observations include an aggregation of minor deviations and/or major deviations from policy or regulatory requirements resulting in probable misstatements or violations that could be significantly detrimental. Immediate corrective action by high-level management will be desirable. Findings in this category will immediately be reported to the appropriate level to ensure timely action can be taken. The design and operating effectiveness of controls evaluated during the audit are not effective and should not be considered reliable.



**III. Observations and Conclusion Summary**

The following table identifies the functional area tested where observations exist, along with the number of observations by risk level. Red reflects audit observations that are considered high risk, yellow reflects audit observations of medium risk, and green reflects observations of low risk.

Internal Audit Area	Auditor's Grade	High	Medium	Low	Page
Removal of Access for Terminated Employee	Needs Improvement	1	-	-	5
Documented Risk Assessment		-	1	-	5
Workstation Lockout Configurations		-	1	-	6
Insufficient Review of Firewall Rules		-	1	-	6
Encryption Key Custodian Acknowledgements		-	1	-	6
Inconsistent Information Security Training		-	1	-	7
Insufficient Policy Documentation		-	1	-	7
Insufficient User Access Reviews		-	-	1	8
<b>Total</b>			<b>1</b>	<b>6</b>	<b>1</b>

**Conclusion Summary**

One High-risk issue was identified during our procedures, and our recommendations for the observations noted provide an opportunity to strengthen internal controls and processes. Our detailed observations and recommendations are described in **Section IV** of this report.

\* \* \* \* \*

We appreciate the cooperation extended to us by various personnel and are pleased to be of service. If there are any questions or comments regarding this report, please contact us. Contact information for the member overseeing this work is presented below.

Scott Nalley, CPA, CIA, CISA  
 Member, Risk Assurance & Advisory Services  
 615-782-4252  
 snalley@kraftcpas.com

#### IV. Observations and Recommendations

**Observation A: Removal of Access for Terminated Employee**

**Risk Level:** High

Access for terminated employees is not always removed timely. During our review of network access within Active Directory, we identified one active user account associated with an Election Commission employee who was terminated in August of 2019. In accordance with the *Tennessee Elections Security Standard*, account access for any departing user must be revoked the same day. However, removal of this account had not been requested by management as of the date of our testing in April 2020 and was being used by another Election Commission employee.

**Risk:** Failure to remove access for terminated employees increases the risk of unauthorized or inappropriate access to voter data, along with increasing the risk of data breaches, resulting in additional financial and reputational risks.

**Recommendation:** Election Commission management should implement a process to ensure that all access is removed for terminated employees on the day of departure to comply with *Tennessee Elections Security Standards*.

**Observation B: Documented Risk Assessment**

**Risk Level:** Medium

The Election Commission does not maintain a formal, documented risk assessment related to security of their information systems. Management maintains an Elections Emergency Response Plan, which contains a limited assessment of risks and mitigation strategies related to operations. However, the Plan does not adequately address information regarding critical assets, including all areas where voter and non-public information is stored, processed or accessed.

**Risk:** Risks associated with the protection and security of voter and non-public information may not be adequately identified and mitigated. As a result, voter information could be compromised, increasing financial and reputational risks.

**Recommendation:** In accordance with the *Tennessee Elections Security Standard*, Management should perform and document, on an annual basis, a risk assessment which identifies critical assets, threats, and vulnerabilities, along with the associated mitigation steps. The risk assessment should consider all areas where voter or sensitive information exists, as well as identify internal and external threats which could result in unauthorized disclosure, misuse, or alteration of voter or non-public information.

**Observation C: Workstation Lockout Configurations**

**Risk Level:** **Medium**

Workstations lockout settings are not configured in accordance with the *Tennessee Elections Security Standard*. Workstations are configured to lockout after 20 failed login attempts, and lockouts are configured with a duration of 15 minutes. In accordance with the *Tennessee Elections Security Standard*, lockouts should be configured with a minimum duration of 30 minutes after six failed login attempts.

**Risk:** Greater login attempts, along with shorter lockout durations, increase the risk of account compromise, which could result in unauthorized access to voter or non-public information, increasing financial and reputational risks.

**Recommendation:** Information Technology Services (ITS) Management should ensure that Election Commission workstations are configured under a separate group policy to enforce lockouts that meet the *Tennessee Elections Security Standard*.

**Observation D: Insufficient Review of Firewall Rules**

**Risk Level:** **Medium**

Management reviews of firewall rules are not performed on a scheduled basis and are not currently documented. Although ITS performs periodic reviews of firewall rules, these reviews are informal and are not performed quarterly in accordance with the *Tennessee Elections Security Standard* requirements.

**Risk:** Firewall rules may not be appropriately or adequately configured to prevent attacks, increasing the risk of unauthorized access to the network or breach of data, resulting in additional financial and reputational risks.

**Recommendation:** ITS Management should ensure that reviews of firewall rules are performed at least quarterly and evidence of review is retained.

**Observation E: Encryption Key Custodian Acknowledgements**

**Risk Level:** **Medium**

Encryption key custodians are not required to formally acknowledge their responsibilities related to key management. In accordance with the *Tennessee Elections Security Standard*, key custodians should formally acknowledge that they fully understand and accept their responsibilities. Although ITS has recently developed a policy related to key management, the policy has not yet been distributed to or acknowledged by the employees responsible for managing and securing encryption keys.

**Risk:** Employees may not be aware of their responsibilities for managing and securing encryption keys, increasing the risk of inappropriate or inadequate treatment, along with increased financial and reputational risk associated with data breaches.

**Recommendation:** ITS Management should ensure all employees charged with managing and securing encryption keys acknowledge their understanding of responsibilities in accordance with the *Tennessee Elections Security Standard*.

**Observation F: Inconsistent Information Security Training**

**Risk Level:** **Medium**

Information security training has not been consistently provided to Election Commission personnel. During our review, we determined that 19 of the 27 Election Commission employees had not formally attended security training in 2019 or in 2020 through the date of our testing, June 2020. Election Commission personnel are provided security training as part of a Metro-wide training program. Also, Election Commission employees are exposed to annual phishing testing, the results of which are reviewed by Election Commission management. However, the frequency and content of training does not appear to meet the intent of the training program required by the *Tennessee Elections Security Standard*.

**Risk:** A lack of consistent and timely information security training increases the risk of inappropriate or unintentional disclosure of voter or non-public information, resulting in financial loss or additional reputational risk.

**Recommendation:** Election Commission management should establish a process to ensure employees receive security training in accordance with the *Tennessee Elections Security Standard*.

**Observation G: Insufficient Policy Documentation**

**Risk Level:** **Medium**

Documented policies do not adequately address cybersecurity or employee acceptable use requirements specific to the Election Commission. Management has adopted certain policies developed and maintained by Metro ITS, including the Information Security and Acceptable Use Policies, along with an internal Elections Code of Conduct. However, the policies do not define requirements that are specifically related to the Election Commission, including approved uses and network locations of technologies, listings of approved products, or responsibilities for all Elections personnel related to information security, which is required by the *Tennessee Elections Security Standard*.

**Risk:** Elections personnel may not be aware of management's expectations regarding information security and acceptable uses of technology, increasing the risk of unauthorized or unintentional disclosure of voter or non-public information, resulting in additional financial and reputational risks.

**Recommendation:** Election Commission management should develop and document cybersecurity and employee acceptable use policies which define requirements specifically related to the management and protection of information stored, used, and processed by the Election Commission. In addition, employees should formally acknowledge their responsibilities related to cyber and information security.

**Observation H: Insufficient User Access Reviews**

**Risk Level:** **Low**

Access reviews performed for all users and their activities within Election Commission systems are not documented. While evidence of review was not available, based on inquiry with management reviews are performed periodically.

**Risk:** Users may have inappropriate or unnecessary access rights, which could result in unauthorized access to voter or non-public information, increasing financial and reputational risks.


**Recommendation:** Election Commission management should ensure that user access reviews are performed and documented in accordance with the *Tennessee Elections Security Standard*, which states that reviews should be performed on a quarterly basis. In addition, reviews should consider access privileges across all Election Commission systems, including but not limited to, Active Directory, PowerProfile, ElectionWare, and EasyVote.

## APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN

---

**METROPOLITAN  
GOVERNMENT OF NASHVILLE  
AND DAVIDSON COUNTY**



DAVIDSON COUNTY ELECTION COMMISSION  
PERMANENT REGISTRATION OFFICE  
POST OFFICE BOX 650  
NASHVILLE, TN 37202  
(615) 862-8800 – Office  
TTY—1-800-848-0298 or Relay 711   
[WWW.NASHVILLE.GOV/VOTE](http://WWW.NASHVILLE.GOV/VOTE)

September 3, 2020

Ms. Lauren Riley  
Metropolitan Auditor  
Office of Internal Audit  
404 James Robertson Pkwy  
Nashville, TN 37219

Re: Audit of Davidson County Election Commission

Dear Ms. Riley,

This letter acknowledges receipt of the interim draft report for the Audit of the Davidson County Election Commission prepared by KraftCPAs. We have reviewed the observations and recommendations. Please find included with this memo our management response. Because this audit included recommendations for Metro ITS, their responses will be by separate communication.

Regards,

A handwritten signature in blue ink, appearing to read "Jeff Roberts".

Jeff Roberts  
Administrator of Elections

c.c. Erica Hightower  
KraftCPAs

---

## APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN

We believe that operational management is in a unique position to best understand their operations and may be able to identify more innovative and effective approaches and we encourage them to do so when providing their response to our recommendations.

	Recommendations	Concurrence and Action Plan	Proposed Completion Date
<i>Recommendations for management of the Election Commission to:</i>			
H	<p><b>A.</b> Election Commission management should implement a process to ensure that all access is removed for terminated employees on the day of departure to comply with <i>Tennessee Elections Security Standards</i>.</p>	<p><b>Accept:</b> We concur. Upon retirement of the employee, the IT Administrator for the Election Commission changed the passwords associated with his account to prevent any continued access and his physical access was revoked. Although the employee’s account remained active, it was only accessible by the IT Administrator of the Election Commission. Because the Election Commission follows the Tennessee Elections Security Standard restricted access philosophy, this employee did not have access to Voter Data. The action taken was limited to only this specific employee because of his unique position. Standard protocol was followed for all other separated employees.</p> <p>This employee served as the Republican Machine Technician during his tenure with the Election Commission. The republican and democratic machine technicians are statutorily mandated positions appointed by the members of the Davidson County Election Commission. Because of the political nature of this position, the Election Commission IT Administrator changed the passwords to this account to prevent any unauthorized or inappropriate access while still being able to monitor email sent to the employee leading up to the Presidential Primary.</p> <p>Future separations of either of these two unique positions will follow the standard protocol. We will work directly with Metro ITS to monitor the email of a separated employee following termination of the account.</p>	Implemented
M	<p><b>B.</b> In accordance with the <i>Tennessee Elections Security Standard</i>, Management should perform and document, on an annual basis, a risk assessment which identifies critical assets, threats, and vulnerabilities, along with the associated mitigation steps. The risk assessment should</p>	<p><b>Partially Accept:</b> We Concur in part. We concur that the Election Commission did not have a single document identifying risks. The Tennessee Elections Security Standard states that county commissions should “perform and document, annually, risk assessments.” The Election Commission performed risk assessments on our most critical assets. These assets are the voting equipment and the voter records. A risk assessment was performed on each of these assets during 2019 where threats and vulnerabilities were considered and mitigation steps identified.</p>	Implemented

**APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN**

	Recommendations	Concurrence and Action Plan	Proposed Completion Date
	<p>consider all areas where voter or sensitive information exists, as well as identify internal and external threats which could result in unauthorized disclosure, misuse, or alteration of voter or non-public information.</p>	<p>The protection of the voting equipment was a primary focus as the Election Commission considered the options for a required move of our voting equipment warehouse in 2019. One of our primary requirements given to Metro General Services in securing appropriate space was the separation of the warehouse from the main office. This requirement was identified after considering the risk of having all of our assets in a single location. The relocation of the warehouse and our requirements for the space were of such significant importance that it was discussed multiple times in our public Commission meetings. The specifications used by the contractor to prepare the new space were identified and approved by the Election Commission as identified in our risk assessment. Examples include, perimeter fencing, monitored alarm, remotely accessible video cameras, removal of all windows, and no roof access. The risk assessment that identified the need for two separate spaces bore fruit in May of 2020 when the main office lost power for a week and we were able to temporarily relocate staff to the new warehouse to prepare for the August election. This was extremely beneficial as the period to accept absentee ballot requests for August opened while the main office was without power.</p> <p>A risk assessment of our voter records was also performed in 2019. Paper copies of voter records are stored behind three doors with each requiring card key access, access is recorded by stored video, and the office is protected by a 24/7 armed guard. Following the physical security risk assessment, the need for additional signage was identified. As a result, we posted notices to the public and other Metro employees that our office is a restricted area and limited to authorized personnel only.</p> <p>Our 2019 risk assessment for our voter records also included a review of the threats and vulnerabilities associated with our electronic voter records. This was especially timely because of our purchase of a new voter registration database. The most significant decision made as a result of this risk assessment was to house the voter registration records on servers with Metro IT instead of contracting with the vendor to store the records. The ultimate decision was made based on Metro IT’s ability to secure the data against unauthorized disclosure, misuse, or alteration of voter data.</p>	



**APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN**

	<b>Recommendations</b>	<b>Concurrence and Action Plan</b>	<b>Proposed Completion Date</b>
		The protection and security of our critical assets is a top priority for the Election Commission. While annual assessments of risks to critical assets are required in the Tennessee Elections Security Standard, the Davidson County Election Commission takes the approach that risks should be constantly evaluated and steps taken to mitigate those risks.	
M	C. ITS Management should ensure that Election Commission workstations are configured under a separate group policy to enforce lockouts that meet the <i>Tennessee Elections Security Standard</i> .	<b>Accept:</b> The settings stated by the auditor are accurate. Metro ITS can configure these settings to those specified in the standard. It is our belief that the settings configured by Metro ITS reduces the chance of automated process of brute forcing the passwords while reducing the chance of account lockouts resulting from a denial of service-based attack. We have compensating controls in place, including monitoring of failed logon attempts with System Center Operations Manager and Microsoft’s Advanced Threat Analytics. Metro ITS will coordinate with the Election Commission to determine how best to configure systems to comply with the Tennessee Elections Standard.	December 31, 2020
M	D. ITS Management should ensure that reviews of firewall rules are performed at least quarterly and evidence of review is retained.	<b>Accept:</b> This finding was accurate at the time of the assessment. Since that time, Metro ITS has developed and implemented a process for conducting this audit on a monthly basis.	Implemented
M	E. ITS Management should ensure all employees charged with managing and securing encryption keys acknowledge their understanding of responsibilities in accordance with the <i>Tennessee Elections Security Standard</i> .	<b>Accept:</b> This finding was accurate at the time of the assessment. Since that time, Metro ITS has developed a process for getting these acknowledgements. Full implementation will be completed by September 7, 2020.	September 7, 2020

**APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN**

	<b>Recommendations</b>	<b>Concurrence and Action Plan</b>	<b>Proposed Completion Date</b>
<b>M</b>	<p><b>F.</b> Election Commission management should establish a process to ensure employees receive security training in accordance with the <i>Tennessee Elections Security Standard</i>.</p>	<p><b>Accept:</b> We concur. Information security awareness training is important to the protection of Election Commission critical assets. Because of a change by Metro of its contractor providing security awareness training, the new program began in November of 2019 and mandated that all employees complete the training by November 2020. Because of the 2020 election cycle, many employees have yet to take the new training mandated by Metro HR. As reflected in Observation F, the security awareness training status of all Election Commission personnel is maintained and monitored by the Metro Human Resources Department. The 27 employees identified in Observation F, must complete the annual mandated training by November 2020 to maintain the frequency requirement mandated by Metro HR.</p> <p>Absent specifics as to frequency and content in the Tennessee Elections Security Standard, the Davidson Co Election Commission will continue to require all staff to complete the required annual training for all Metro employees and we will also continue to supplement this training with internal communications to ensure that Election Commission employees are knowledgeable of all threats.</p>	November 1, 2020
<b>M</b>	<p><b>G.</b> Election Commission management should develop and document cybersecurity and employee acceptable use policies which define requirements specifically related to the management and protection of information stored, used, and processed by the Election Commission. In addition, employees should formally acknowledge their responsibilities related to cyber and information security.</p>	<p><b>Partially Accept:</b> We Concur in part. The Metro Information Security Policy specifically speaks to approved uses and network locations of technologies. In signing the Acceptable Use Policy, employees acknowledge they understand their access and use “shall be limited to the Information Technology Assets necessary and appropriate for the User to perform the job duties and functions assigned to him or her.” All employees also acknowledge a “User shall not access Sensitive Information from a Device other than the one issued to the User by the Metropolitan Government or an Approved User Owned Device.” The connection of Metropolitan Government Issued Devices can only be accomplished via Metro ITS ticketing protocol. As defined in the Policy, Metro ITS or the Election Commission’s IT staff shall coordinate the relocation and modification of Information Technology Assets “including, but not limited to, network equipment, software, and peripherals. While there is not a list of approved products, Election Commission employees are prohibited from installing any products without approval from the Election Commission IT Administrator.</p>	Implemented

**APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN**

---

	Recommendations	Concurrence and Action Plan	Proposed Completion Date
L	<p>H. Election Commission management should ensure that user access reviews are performed and documented in accordance with the <i>Tennessee Elections Security Standard</i>, which states that reviews should be performed on a quarterly basis. In addition, reviews should consider access privileges across all Election Commission systems, including but not limited to, Active Directory, PowerProfile, ElectionWare, and EasyVote.</p>	<p><b>Accept:</b> We concur. Although periodic reviews are the current practice, user access reviews will be performed and documented quarterly in the future.</p>	<p>Implemented</p>