The Rundown podcast transcript for Performance Audit report titled ***Reviewing Kansas's Procedures for Election Security, Part 2*** – Released July 2023

Brad Hoff, Host and Recruiting and Training Manager: [00:00]
Welcome to The Rundown, your source for the latest news and updates from the Kansas Legislative Division of Post Audit featuring LPA staff, talking about recently released audit reports and discussing their main findings, key takeaways and why it matters. I'm Brad Hoff. In July 2023, LPA released part two of a performance audit examining Kansas' Election Security Procedures. I'm with Andy Brienzo, principal auditor at Legislative Post Audit who supervised the audit. And also joining us are Mohri Exline and Sam Dadds, senior auditors and team members. All of you, Welcome to The Rundown.

Andy Brienzo, Supervisor and Principal Auditor: [00:40]
Thanks Brad.

Mohri Exline, Team Member and Senior Auditor: [00:40]
Thanks Brad.

Sam Dadds, Team Member and Senior Auditor: [00:41]
Thank you, Brad.

Brad Hoff, Host and Recruiting and Training Manager: [00:44]
Now, before we get into the audits findings, describe what you looked at for this audit and how it relates to part one, which LPA released back in February of 2023.

Andy Brienzo, Supervisor and Principal Auditor: [00:56]
Okay, so initially this was part of a five question proposal that was approved by the Legislative Post Audit Committee. We split it for reporting purposes into two different parts, as you mentioned. So, part one dealt with the original questions - three through five of the proposal. So, that dealt with training for county election officers and election workers cast vote records, ballot images and security, issues

related to long-term care facilities. This report, part two, deals with questions one and two from that initial proposal, which actually for this we combined into a single question. So, this will look at whether county election offices have adequate policies and practices to ensure the accuracy and security of specifically of voting machines, ballots, storage units and devices used to tabulate votes during elections. There's a lot of other areas that are important for election security that we didn't get into just because the scope didn't include them, the audit proposal didn't include them, but this is part of a larger five question proposal that was approved.

Brad Hoff, Host and Recruiting and Training Manager: [02:03]

So, to set the stage for the rest of our discussion, talk a little bit about the different types of people and machines that are involved in county's elections.

Sam Dadds, Team Member and Senior Auditor: [02:16]
Okay. So, in Kansas, elections are overseen by the county election officers and 101 of those counties that duty falls to the elected county clerk, but in Johnson County, Sedgwick, Shawnee and Wyandotte County, the election commissioner oversees the elections and that election commissioner in those counties is appointed by the Secretary of State. The major difference between the county clerk and the election commissioner is the clerk is also responsible for all of their other duties, tied to their position, such as tax assessments, while the election commissioner is only responsible for overseeing elections. So, the election officers also rely on their staff and election workers to help run elections. There's also different types of machines that are used, during the election process. I believe the ones people are most concerned about are the ballot marking devices and the vote tabulation machines. So, the ballot marking devices or the voting machines are used by voters to cast and print their ballots and the tabulation machines are optical scanners that are used to scan and record the votes on the paper ballots. These can be used at the polling places or they can be centrally located depending on the choice of the county. So, the last type of machine that's used during the election process is the election management system and this serves to aggregate all of the vote totals from across the county and finalize the election.

Brad Hoff, Host and Recruiting and Training Manager: [03:48]
Now in reading the report, it looked like the team relied mostly on federal level best practices to evaluate counties, policies and practices. What types of things do these practices cover and how do they compare to state law?

Mohri Exline, Team Member and Senior Auditor: [04:04]
Right. So, we reviewed best practices from the US Election Assistance Commission, which is also known as the EAC. This is the federal agency that tests and certifies voting machines nationwide. So, of these best practices, we selected 50 practices that we thought were likely to be important for most counties security and so these practices fell into five main categories. You can see a full list of those best practices in

appendix B, and so we'll just go through each of those five categories really quick. So that first category is overall process security. So, this refers to basic practices that just kind of set the stage for a secure election. So, these are things like buying certified election equipment, maintaining an inventory of this equipment, and then also just tracking everything that happens with it. The second category is election management computer security. So, this refers to securing this actual computer so that it will accurately compile countywide results. So, this category included things like limiting physical access to the computer and then also logging computer activity and then also keeping it disconnected from the internet. The third category is ballot security. So, this refers to things that are done to track ballot activity, such as noting how many ballots are sent from the county election office to the polling places, and then it also is, you know, comprehensively tracking how they're used and using controls to ensure that all of those legal ballots are tallied. The fourth category is voting and tabulation machine security. So, this refers to securing these machines so that they'll accurately reflect voters choices on election day. So, this includes things like testing them before elections and then also securing them during storage. The final category is transfer and movement security.

This refers to securing election equipment as well as election results, media and ballots during transfer to and from the county office in the polling places, and then also sealing equipment and election results during that transfer. So, one of the first things that we did was also review state law and regulations, and then we found that state law and regulations were generally more general than the best practices. They fully reflected eight and partially reflected three of the 50 best practices that we focused on. So, for example, state law actually requires voting and tabulation machines to be EAC certified, but the best practices went a step further with that and they actually specified things like that these machines should have software that comes from a trusted source. State law did include five additional election security requirements that were not originally included in the best practices from the EAC. So, these were things like post-election tests. There were a few other things as well, and we went ahead and added those to our requirements into our best practices for a total of 55 best practices.

Brad Hoff, Host and Recruiting and Training Manager: [07:45]
The team selected 15 counties for review, but ran into some issues with two of them. Talk about what specifically you looked at, why did you choose those counties and what kinds of problems did you encounter?

Andy Brienzo, Supervisor and Principal Auditor: [08:03]
So, as you mentioned, two of them we had issues with, I'll get to those in a minute, but the 13 that we actually were able to fully review, are Chautauqua, Dickinson, Douglas, Harvey, Jackson, Johnson, Lincoln, Miami, Riley, Russell, Sedgwick, Sheridan and Wyandotte counties. So, we chose them because they varied in in areas like geographic locations. So, we had, you know, counties that are from all over the state. The number of voters, so we had counties that had just, you know, a couple

thousand voters all the way up to Johnson County, which has hundreds of thousands of voters and then the types of election or the types of voting machines they used. So, we chose ones that used voting machines from different vendors. Sheridan's unique in that it doesn't use voting machines. They make them available to comply with federal law, but they aren't typically used in elections. So, they are kind of unique in that respect. They also hand count their ballots and don't use a tabulating machine or an election management computer system. So, they're quite unique and that's why we chose them. So, the two others, that we had issues with were Chase County and Ford County. So, we could review their policies, but we couldn't verify their practices because they sealed most of their 2022 election documentation. So, for each county, we intended to review their written security policies and then any available documentation that they had on hand to verify whether, you know, in 2022 during either the primary or general elections, they actually followed those security policies so we could verify what they were doing in practice. But Chase and Ford County, unlike the other 13 that we looked at, they sealed most of this documentation, and they put it into the containers that they put their ballots in. So, this is Legislative Post Audit has very wide-ranging documentation access, but the one, pretty much the one thing that we can't get into are ballot bags, sealed ballot bags. State law requires that sealed ballots remain sealed and so since all of their documentation, or a lot of it was in these ballot bags, we simply couldn't review enough to get a thorough understanding of what their practices were in 2022 and draw conclusions. The other thing I'll mention is that Ford County officials were the one county, of the 15 that didn't let us inspect their election management computer. So, the other 14, including Chase County, when we were on site, when we visited all of these counties, we were able to inspect their computer, see if it was connected to the internet, see what kind of software was running on it, and Ford County was the one county that didn't let us do that.

Brad Hoff, Host and Recruiting and Training Manager: [10:45]
Now, before we get into the results of the audit and your review, talk a little bit about the methodology the team used and any important caveats that the team outlined in the report that will help the reader better understand the work that the team completed during this audit.

Andy Brienzo, Supervisor and Principal Auditor: [11:05]
Okay. So, the first thing we did really was talk extensively to county officials and spend time on site, actually at all 15 counties, including Chase and Ford, inspecting their election offices, inspecting their storage facilities, walking through sort of the layouts and the particular controls that they had in place that we were able to observe. We also reviewed any written security policies that they had available. Sam's going to talk a little bit later about the results of that particular, review and as I said, any available documentation to verify what these counties did in practice in 2022. And as I said, Chase and Ford, we had some limitations, with both of those counties. Some of our conclusions are based on non-projectable samples of voting

and tabulation machines or polling places because we just didn't have time or resources to review all the machines and all the polling places in all of these counties. Johnson County, for instance, has 2,000 machines and 150 polling places and so that county alone has way too much for us to review given our resources. We think the samples are sufficient to reveal problems with the design or execution of their security controls, but because we didn't review all the machines or the polling places, there could be some additional control weaknesses that could potentially exist that we just weren't able to see in our samples. And our conclusions are based on either the documents counties provided or our own observations that we made during those site visits. So, there were cases where county election officials told us they had controls in place during the 2022 elections that would've aligned with our best practices, but they couldn't provide documents or show us something that we could observe during our visit. So, it's possible that there are cases where these counties did indeed follow best practices in 2022, but weren't counted as having done so because we couldn't, we just couldn't verify it. We don't know how common that might have been. We also didn't evaluate whether the counties' controls actually worked as intended. So, an example of this would be we reviewed whether counties kept lists of the people who were given keys to secure storage facilities where things like voting machines, tabulation machines are being stored, but we didn't determine whether the lists were limited to only the appropriate staff. So, we can conclude on whether the counties have the control in place. So, the control is intended to track who has access to the machines, but we didn't evaluate whether they've appropriately limited that access as part of our work. The other thing that I want to point out I think is really important is that we didn't evaluate whether the 2022 elections in these 15 counties were correctly tabulated or whether they accurately reflected the will of the voters because that stuff was outside of the scope. I also want to make clear that we focused on the 2022 elections. We did not focus on 2020. We talked to county officials about what types of documentation might be available, but by the time we started, the 2020 documentation was either sealed or destroyed, in alignment with state and federal law and the approved audit scope did not include a lot of other stuff that helps ensure that elections are secure. So, this is stuff like voter registration, mail-in voting ballot, drop boxes, the post-election auditing process. These are all elements of election security that simply fell outside the audit scope. And in any cases where that stuff is in place, you know, robust security practices are in place in those areas that would simply compliment and back up the things that we are discussing in this report.

Brad Hoff, Host and Recruiting and Training Manager: [14:46]
The report notes that counties generally had adequate practices in the first two areas you reviewed, those were their overall process and election management computer security. Tell me more about these areas.

Sam Dadds, Team Member and Senior Auditor: [15:03]
So the first, the first two areas of five, if you're reading the report, we have a figure for

each one of the five areas, scattered throughout the report. Within each relevant section that breaks down results for each county, if you're following along, for overall process and election management security, these areas include basic practices that set counties up for a secure election. So, the counties we reviewed generally had strong practices for ensuring only trusted software was installed on the machines and that paper ballots were available to confirm election results. However, counties inventorying practices weren't as strong as a whole, but they were generally adequate. To give you an example of a strong inventory system, Douglas County uses a scanning system to automatically log each time a piece of voting equipment leaves or returns to their warehouse. Conversely, Russell County doesn't log when their equipment leaves or returns to their warehouse. And for election management computer security practices, of the 13 counties, we reviewed, they also generally had adequate security practices with only a few exceptions. So, the best practices in this category help ensure that the election management computer is secured and will accurately aggregate the countywide results. So, all counties demonstrated strong practices for ensuring that their election management computers can't be used for other purposes. And most of them also had strong practices for ensuring activity on those computers as monitored, and that they're secured from unauthorized access. So, to give you an example of counties that were doing well, Douglas, Johnson, and Wyandotte, they had advanced election management computer security. Their computers were locked in video monitored rooms requiring key codes or badge access to get in. The computers also required complex passwords and logged all system activity. Some common control weaknesses in the area related to counties' practices for physically securing their computers. This typically was due to the size of the counties. They had limited space and limited resources. Many smaller and medium-sized counties had to make do with existing space in their county courthouses instead of being able to have, secured rooms devoted to their election management system. So, to give an example, counties like Chautauqua and Lincoln, are relatively small counties and they use laptop systems rather than, the permanent desktop systems we saw in places like Douglas, Johnson and Wyandotte. So, while we were there on site, we were able to view and observe that the laptops were kept locked up, but what we couldn't do is review their processes of how they keep those machines secured on election night because we weren't there. However, these smaller counties did well on things like monitoring their computer access, logging the activity, and requiring complex passwords in order to log on. So, and of the systems, we were able to review, we were able to see that none were connected to the internet and nor did they have any non-election related software installed on them.

Brad Hoff, Host and Recruiting and Training Manager: [18:23]
Now, the other three areas that you looked at weren't as strong as the first two that, that Sam had had just talked about. The team found counties had weaker ballot security practices, generally inadequate voting and tabulation machines, security practices and inconsistent transfer and movement security practices. Talk a little bit

more about what you found in these three areas.

<u>Mohri Exline, Team Member and Senior Auditor:</u> [18:54]
So, the best practices in the ballot security category, track ballot activity and help ensure that invalid ballots aren't counted. So, as figure four shows in the report, many counties had most of the ballot security practices that we reviewed, however, they were generally weaker than the first two areas that Sam addressed. For instance, about half of those counties we reviewed had weak ballot accounting practices. So, these varied from county to county. One example of good processes was in Dickinson County where they documented how many ballots were sent to each polling place and included tracking voted, provisional, spoiled, and unused ballots. They also documented how many voters used voting machines. Many counties missed this latter step, which is important because it shows how many paper ballots should have been used. Counties did sometimes create standardized forms that could be effective as ballot security controls. However, in many cases, forms weren't filled out completely or correctly. So, for example, in Sedgwick County, they created a form that required polling places to balance the numbers of checked-in voters to the number of used ballots each hour. But many polling places were missing all or pieces of this documentation. So, in terms of voting and tabulation machine security, most of the 13 counties that we reviewed had inadequate security practices except for physical security practices. So, the best practices in this category help ensure that voting and tabulation machines are secure and that they accurately reflect voters choices on election day. So, looking at figure five in the report, you can see that most counties had adequate practices for physically securing their election equipment while in storage. However, counties had weak practices for testing this equipment at the time of purchase or before or after elections. So some examples of this, counties like Douglas, Harvey, Johnson, Riley, Sedgwick, all stored their voting and tabulation machines in locked video monitored rooms. These counties also required that staff scan their badges to enter, or in the case of Harvey County, there was a fingerprint scanner used instead. However, in terms of testing, many counties didn't provide documentation showing that all of their electronic equipment had undergone acceptance testing when it was purchased. These tests ensure that they are receiving equipment that is intact and correctly functioning when they first buy them. We also found problems with most counties' logic and accuracy testing. This logic and accuracy testing happens prior to elections to ensure that electronic machines are working prior to those elections. So, for example, Chautauqua, Dickinson, Jackson, Lincoln, Riley and Sheridan counties didn't provide documentation showing that they conducted logic and accuracy testing on all of the machines that we sampled. So, finally, in terms of our last category of transfer and movement security, we found that counties were lacking in controls in terms of security practices that would help ensure that electronic equipment, election results, media and ballots are secure when transferred to and from the county election office and polling places. So, looking at figure six in the report, we can see that most counties had stronger practices for monitoring

equipment deployment to polling places and ensuring that election results were secured during transfer back to the election office. However, they had inadequate policies for monitoring that equipment was secure at the polling places and safely returned after the election. So, one example of this, Johnson County tracked when and by whom all election equipment, paper ballots, election results, media and other supplies were transferred to and from the polling places. So, some counties created standardized forms that they said recorded transfer of materials and machines, but it wasn't always clear what the forms were meant to document. So, for instance, Jackson, Lincoln, Miami and Russell counties provided chain of custody documents that had signatures, but it wasn't evident what signatures were attesting to.

Brad Hoff, Host and Recruiting and Training Manager: [23:39]
What do you think explained the differences you saw across the counties you reviewed?

Mohri Exline, Team Member and Senior Auditor: [23:47]
So, there are a few things that we saw that, could explain some of those differences. One of the biggest ones was county size and resources. This played a large role in these differences. We could see that larger counties generally followed more of the best practices that we reviewed than smaller counties did. So, looking back over those results, we see that all seven of the large counties we reviewed had adequate security practices in 10 or more of the areas that we reviewed. On the other hand, only three of the small counties that we reviewed had adequate security practices in ten or more of the areas that we reviewed. So, larger counties generally have stronger security practices than smaller counties because the sheer volume and complexity requires larger counties to have more controls and better documentation to ensure that things aren't missed. Larger counties also have more financial and staff resources to dedicate to elections. So, beyond size, insufficient guidance and oversight at both the state and county levels likely contributes to a lack of controls. So, the state doesn't appropriate funding to help counties pay for election security. Further, the Secretary of State doesn't proactively provide state level guidance or make recommendations about minimum security expectations. The annual training that the Secretary of State's office provides county election officers is high level and doesn't get into topics of like the importance of security controls or how to adequately design and practice them. So, finally, county election officers may not be adequately training county election workers or holding them accountable for following established practices. So that being said, election workers may not understand security control's importance or how to correctly carry them out. So, standardized forms across counties of all sizes that were filled out incorrectly or not at all are examples of this happening.

Brad Hoff, Host and Recruiting and Training Manager: [25:59]
The team also looked at county's election security policies. What did you find in this area?

Sam Dadds, Team Member and Senior Auditor: [26:06]
Well, in short, we found that none of the 15 counties we reviewed had comprehensive written election security policies or guidelines. The county officials told us that they rely on state law and the election standards handbook provided by the Secretary of State's office. Many counties did have a few standardized forms and checklists that they used to help guide certain processes, but the quality and completeness varied across counties and because elections are a complicated process, we expected to see each county have a regularly updated policy manual outlining the county election officer's to help with election worker training and election officers succession.

Brad Hoff, Host and Recruiting and Training Manager: [26:50]
And finally, what's the main takeaway of this audit report?

Andy Brienzo, Supervisor and Principal Auditor: [26:53]
So the EAC lays out what is really an ideal system of security practices. Many compliment one another, provide redundancy for one another. So, if one practice is missing, others may be in place that will help secure the same area. Kansas' decentralized election structure across 105 counties also helps inherently to provide some security. So, each county has different processes, controls, they use different vendors, things like that. So, impacting a statewide election would require defeating controls in multiple counties, each of which operates differently. So, the EAC provides good practices that are a good goal to strive for. Having them all in place would be great. It would bolster counties election security, but it's not realistic to think that every county would have all of them in place. And like I said, there are other things that are mitigating any weaknesses that we found. I think the overall takeaway from this audit is that there are opportunities for counties and especially the Secretary of State's office and the Legislature to help counties bolster their processes. So, these are complicated, complicated processes. They're expensive, they happen infrequently. A one size fits all approach doesn't make sense, but greater state level support and financial resources, templates, things like that would help counties maximize the security of their elections.

Brad Hoff, Host and Recruiting and Training Manager: [28:19]
Andy Brienzo is a principal auditor and Mohri Exline and Sam Dadds are senior auditors at Legislative Post Audit. They completed an audit examining Kansas' election security procedures. Andy, Mohri and Sam, thanks for joining me.

Mohri Exline, Team Member and Senior Auditor: [28:33]
Thank you, Brad.

Sam Dadds, Team Member and Senior Auditor: [28:35]
Thanks Brad.

Andy Brienzo, Supervisor and Principal Auditor: [28:36]
Thank you.

Brad Hoff, Host and Recruiting and Training Manager: [28:37]
Thank you for listening to The Rundown. To receive newly released podcasts, subscribe to us on Spotify or Apple Podcast. For more information about Legislative Post Audit and to read our audit reports, visit kslpa.org. Follow us on Twitter @ksaudit or visit our Facebook page.

General Considerations/Copyright

The information in this podcast is not protected by copyright law in the United States. It may be copied and distributed without permission from LPA. LPA should be acknowledged as the source of the information. Listeners may not use this information to imply LPA endorsement of a commercial product or service or use it in a way that might be misleading.