KANSAS LEGISLATIVE
DIVISION of
POST AUDIT

A Performance Audit Report Presented to the Legislative Post Audit Committee

Information Systems: Reviewing Specific IT Security Controls Across State Agencies and School Districts

July 2023

Report Number: R-23-006

Introduction

K.S.A. 46-1135 authorizes our office to conduct information technology (IT) audits as directed by the Legislative Post Audit Committee. These audits are conducted on a 3-year cycle. During its December 2022 meeting, the Committee approved a proposal to change the format of our IT audits. This year we will review multiple agencies at the same time, on select IT security controls and issue public reports. Our previous audits were in-depth reviews of IT security at individual agencies, that resulted in confidential reports. The Committee also approved inclusion of a handful of school districts as part of the IT audit work.

Objectives, Scope, & Methodology

Our audit objective was to answer the following question:

1. Do selected state agencies and school districts adequately comply with certain information technology security standards and best practices?

We selected 12 state agencies and 3 school districts as part of this audit. We chose 15 IT security controls across 3 IT control areas. Those areas were Security Awareness, Account Security, and Incident Response. Aside from 2 best practices, we evaluated IT controls already codified in the state's security policy.

We focused on entities' security posture at the time of the audit. Our onsite fieldwork was staggered across the entities, starting on January 25, 2023 and ending April 12, 2023. To assess compliance, we interviewed staff, reviewed relevant policies and procedures and evaluated relevant computer settings. We reviewed security awareness training and other applicable documentation as necessary. Lastly, we conducted or evaluated social engineering tests. Those tests included email phishing campaigns, as well as trash and clean desk checks.

We limited our work to a small number of IT areas and a handful of controls. At times, we were unable to test all selected requirements. Because we did not do a more comprehensive review, other security control weaknesses may exist that represent unknown risks.

Additionally, some work included samples. We generally drew samples randomly, but at times we used judgmental sampling. Results from that work cannot be projected. However, problem findings identified as part of that work represented security threats which in and of themselves provided us with reasonable assurance that problems existed.

More specific details about the scope of our work and the methods we used are included throughout the report as appropriate.

Legislative Post Audit Committee rules require us to report when an agency fails to respond to a recommendation or responds negatively. The Department of Education

rejected our recommendations.

Important Disclosures

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. Overall, we believe the evidence obtained provides a reasonable basis for our findings and conclusions based on those audit objectives.

Audit standards require us to report confidential or sensitive information we have omitted when circumstances call for that. In this report, we summarized IT security findings across 15 entities. Readers may have expected to see findings attributed to individual entities. As agreed to by the Committee, we avoided attributing findings to specific auditees to avoid reducing their security posture further. Finally, we decided to make entity-specific audit documentation confidential under Kansas Open Records Act exemptions K.S.A. 45-221(a) (12) & (45).

Audit standards require us to report our work on internal controls relevant to our audit objectives. They also require us to report deficiencies we identified through this work. Because the scope of this audit was to evaluate selected information security controls, our planning, fieldwork, and the final report are designed to meet these standards.

Our audit reports and podcasts are available on our website (www.kslpa.org).

More than half of the 15 entities we audited did not substantively comply with selected IT standards and best practices.

Background

State agencies must follow Information Technology Executive Council (ITEC) security standards to protect sensitive information against data loss or theft.

- Many Kansas agencies collect sensitive data on taxpayers and citizens. This data can include tax records, criminal records, and health care information. Several agencies maintain confidential information that have significant penalties for loss or disclosure.

- Kansans depend on governmental agencies to protect their personal information. For this reason, it's important state agencies adhere to strict IT security policies and procedures.

- The Legislature created the Information Technology Executive Council (ITEC) in 1998. State law (K.S.A. 75-7203) requires ITEC to adopt information technology resource policies and procedures for all state agencies.

- ITEC created various policies, including policy 7230A on IT security standards. This serves as the state's official IT security policy. That policy governs "all Kansas branches, boards, commissions, departments, divisions, agencies and third parties used to process, transmit or provide business capabilities on behalf of Kansas state government." In other words, all state agencies must adhere to the IT security policy. IT security standards generally include requirements for policies and procedures. They also include requirements for physical, system, and application controls. These controls reduce the risk that confidential data is compromised, lost, or stolen.

- The state's IT security policy is similar to security standards put out by other organizations. The National Institute of Standards and Technology (NIST) standards come from the federal government. The Center for Internet Security (CIS), and the International Organization for Standardization (ISO) both produce standards that are used widely throughout the world.

- Some state agencies may be subject to additional state or federal laws to protect sensitive data. For example, the federal Health Insurance Portability and Accountability Act (HIPAA) requires entities to protect relevant health information. The Internal Revenue Service (IRS) imposes extensive security guidelines for entities that maintain tax data.

In an effort to improve IT security compliance statewide, the 2018 legislature passed the State's Cybersecurity Act in 2018.

- It pertained to most executive branch agencies with a few exceptions. Elected office agencies, the Adjutant General's department, the Kansas Public Employees Retirement System, the regents' institutions (universities), and the Board of Regents were exempted. It did not cover judicial and legislative agencies.

- It created the Kansas Information Security Office (KISO) as a separate state agency to administer the Act. KISO helps agencies develop cybersecurity programs that follow state and federal security standards. KISO also provides a cybersecurity training program at no cost to the agencies. KISO is led by the state's Information Security Officer (CISO), who helps coordinate cybersecurity efforts between agencies.

- It codified cybersecurity service costs. The Act allowed agencies to pay for cybersecurity services from several sources, including fees. It also allowed KISO to charge agencies for certain security-related functions. Resulting fees were to be used for cybersecurity purposes.

- It clarified that agency heads remain responsible for their agency's security postures. Agency heads have several specific responsibilities. Those include the following:

    - ensuring an agency-wide information security program is established;
    - designating an information security officer;
    - taking part in annual agency leadership training on specific cybersecurity-related topics;
    - notifying the state's CISO about breaches within 48 hours after discovery; and
    - submitting a cybersecurity report to the CISO every 2 years.

In 2023, the legislature passed House Bill 2019 which strengthened or added components in the 2018 Cybersecurity Act.

- It required all public entities experiencing a significant cybersecurity incident to notify KISO within 12 hours of discovery. For purposes of reporting security incidents, the law defined a public entity as any public agency of the state or political subdivision. As such, school districts, counties, cities, and similar governmental entities were included. The law defined significant cybersecurity incidents as those that "result in or likely result in financial loss or demonstrable harm." The law also established incident notification requirements for government contractors, election data, or criminal justice data.

- It required KISO to perform confidential audits of executive branch agencies. Those audits should cover applicable state and federal laws, rules and regulations, executive branch policies and standards, as well as ITEC policies.

- The Act required KISO to make a cybersecurity awareness training program available to all branches of state government. Previously, the law required KISO to provide awareness training only to executive-branch agencies at no cost. The law also removed the requirement to make the training available free of charge.

- It added 2 new controls agency heads are responsible for: disabling login credentials on the day employees depart, and ensuring employees with access to IT systems get at least 1 hour of IT security training.

Local entities are not required to follow the state's IT security policy to protect sensitive information against data loss or theft.

- Local entities such as school districts or city and county governments also collect sensitive data on Kansans. This data can include K-12 student records, tax records, and health care information.

- As mentioned earlier, the Legislature created the Information Technology Executive Council (ITEC) in 1998. State law (K.S.A. 75-7203) requires ITEC to adopt information technology resource policies and procedures for state agencies.

- The state's IT security policy created under ITEC authority does not apply to local governments including school districts. Local entities may be subject to other state and federal laws to protect sensitive data. For example, the federal Family Educational Rights and Privacy Act and the Kansas Student Data Privacy Act restrict who districts can release certain student data to. But neither law requires school districts to implement specific IT security controls.

- The Kansas State Department of Education (the state's oversight agency for Kansas' 286 school districts) also does not require school districts to implement specific IT security standards. Our 2021 audit on school districts' self-reported IT security practices found many districts did not follow basic security standards. In response, the department took several actions to help improve districts' IT security processes. These actions included the following:

    - creating a K-12 technology council (members were working on developing best practices and a how-to toolkit);
    - creating an IT technology webpage (includes resources, training materials, and a link to the department's IT policy handbook);
    - making security awareness training available to all districts at no cost; and
    - providing districts with templates districts should consider when developing security policies.

    However, the department stopped short of requiring districts to follow a minimum set of security standards.

State and local entities must balance business risks against security risks.

- Government entities across the nation are targets of data breaches because they maintain valuable information. Several Kansas-specific security incidents are listed below:

    - In March 2023, the Newton School District (USD 373) in central Kansas detected a network security incident. The district had to shut down school operations for 2 days. As of March 29, news reports described the incident as an ongoing investigation.

    - In April 2022, the Wyandotte County Unified Government suffered a ransomware attack on several computer systems. Email, human resources, and the county's mapping systems were all affected. According to a news report 6 months after the incident, officials still did not have a clear explanation of how the attack occurred.

- Generally, state agencies and local entities may prioritize their core mission over information security. Agencies focus on their core missions such as collecting taxes, issuing various types of licenses, or protecting the state's natural resources. School districts' missions center on educating children from kindergarten through 12th grade.

- Implementing security controls takes staff, time, and resources. Security controls often can reduce staff speed or limit functionality. This creates a conflict between business needs and security risks.

- Entities must understand and evaluate their security risks to make informed decisions how to best secure their data, while carrying out their primary missions.

Our IT audits continue to help evaluate the state's IT security posture.

- Except for the IT security audits conducted by our office, there are no external evaluations of agencies' security practices to ensure they comply with ITEC security standards.

- Since 2014, our office has produced IT security audits on many state agencies. Individual audits were kept confidential under K.S.A. 45-221(a)(12) because their information could jeopardize agencies' security.

- Our office produced public 3-year summary reports in December 2016 (20 agencies), February 2020 (19 agencies), and most recently in December 2022 (21 audits on 20 entities).

- Since 2020, the Legislative Post Audit Committee (LPAC) approved adding a small number of school districts to our audit work. This mandate continued in the current 3-year plan (2023-2025).

- During its December 2022 meeting, the Committee asked us to conduct more limited-scope IT audits for multiple agencies at the same time. Results would be released in a public report, issued 2-3 times a year.

Method

We audited 15 entities on selected controls related to Security Awareness Training, Account Security, and Incident Response.

- The full list of 15 entities we audited can be found in **Appendix B.**

    - We selected 12 state agencies based on their inherent risk scores and a lack of previous audit. Specifically, agencies had to have a risk ranking of 'medium' or higher (a scoring system we created based on the type and amount of confidential data agencies maintain, as well as other factors). Second, we selected agencies that had never received an IT security audit from us, or had not been audited by us in at least 4 years.

    - We selected 3 school districts because of their willingness to undergo an audit. In 2021, we conducted a survey of 42 larger school districts to learn which ones were willing to receive an IT security audit. The 3 districts we selected had "opted in" on the survey and were located across the state.

- We evaluated the entities' compliance across 3 subject areas: Security Awareness, Account Security, and Incident Response. We limited our audit to these areas because our past audits showed agencies struggled to comply in those areas. They also presented a mix of technical and non-technical subjects which helped us stay within legislative time constraints.

- We evaluated 5 controls in each subject area, for a total of 15 controls. Controls are a type of requirement, which if followed, help strengthen entities' information security. We selected these controls because they are generally accepted in the industry as foundational to an entity's IT security posture. 13 of the 15 controls came directly from the state's security policy (ITEC 7230A). We added the other 2 controls from other security standards because we thought they were sufficiently important to round out our audit program.

- It's important to remember that the state's IT security policy 7230A has 13 areas and nearly 120 controls in total. Other standards issued by the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) are larger and more complex. For example, CIS has 18 control areas and over 150 controls.

- As mentioned previously, Kansas school districts are not subject to the state's IT security policies. Similarly, KSDE doesn't impose other security standards on districts. However, KSDE has suggested a security standards template for school districts to consider. That document is similar to the state's security policy. As a result, we felt comfortable evaluating school districts against the same 15 controls.

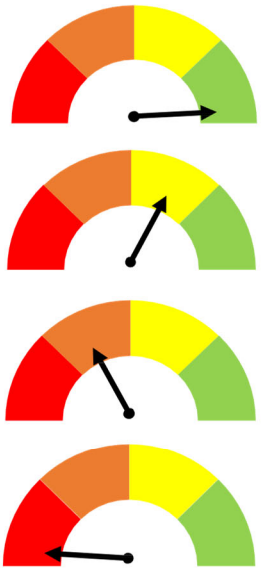
We followed previously established scoring processes during this audit to evaluate entities' security compliance.

- In our prior IT security audits, we developed a robust process to score entities' performance within each control area. Although we only audited 3 areas in this audit, we decided to use the same scoring method:

    - We awarded between 0 and 3 points for each control we evaluated. Generally, we awarded 3 points for full compliance and 2 points when the entity was mostly compliant. We awarded 1 point when the entity had taken initial steps towards compliance, and 0 points if the entity had no process in place to adhere to the requirement.

    - The resulting points in each area were converted to a percentage which fell into 1 of 4 possible quadrants. **Figure 1** shows the possible results.

Figure 1. Categorization of Results For 3 Audited Control Areas



Green indicates 76%-100% compliance. This means **minor/no control issues** within the audited area.

Yellow indicates 51%-75% compliance. This means **moderate control issues** within the audited area.

Orange indicates 26%-50% compliance. This means **major control issues** within the audited area.

Red indicates 0%-25% compliance. This means **significant control issues** within the audited area.

Source: LPA methodology.

- We set the cutoff for substantial compliance at 50%. Agencies scoring above 50% (yellow and green) were considered to have substantively complied in that area. It should be noted this was a fairly liberal threshold. Agencies scoring yellow or green generally still had findings to work on.

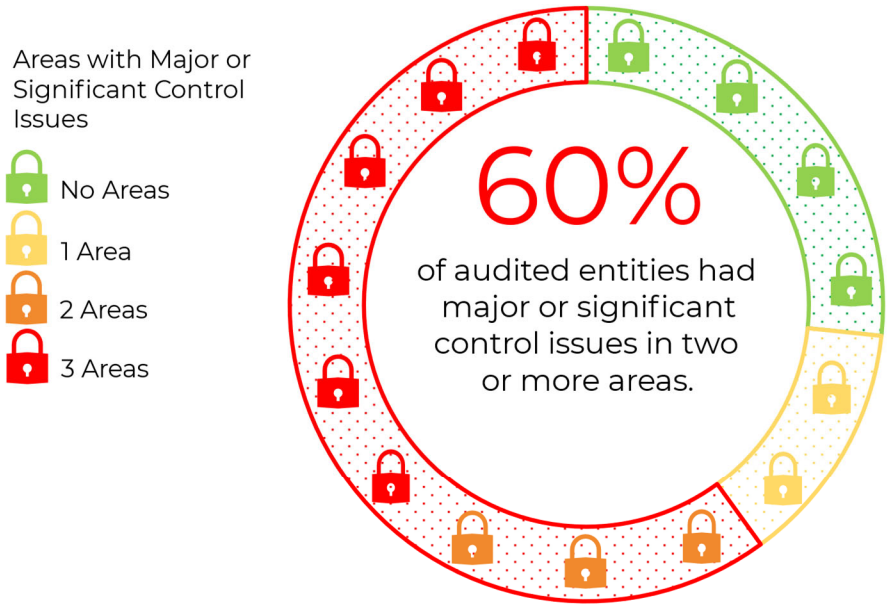
Overall Outcomes

9 of 15 entities did not substantively comply with IT standards and best practices in at least 2 of 3 subject areas we evaluated.

- We expected entities to comply with the controls we evaluated because they were state requirements or generally accepted industry best practices.

- 6 entities scored 50% or less in all 3 areas we evaluated. Another 3 entities scored 50% or less in 2 of 3 areas. **Figure 2** shows the entities' performances across the three areas. As the figure shows, only 4 entities scored more than 50% in all 3 areas. 2 entities scored more than 50% in 2 of the 3 areas we evaluated.

Figure 2. Nine of fifteen entities did not substantively comply with selected IT security controls in two or more areas.



Source: Summary of LPA analysis of selected IT security controls at 15 entities.

- Only 1 entity received a score of 100% in any area. This is noteworthy because most controls we evaluated were ITEC standards that had been in place since at least 2019.

- When entities don't have adequate security controls, the risk increases that their confidential data is lost or stolen. This can occur when entities have a significant security incident or when they are unable to adequately recover from a service disruption. Entities can also face financial penalties and reputational damage when their confidential data is compromised.

- Based on our interactions with staff, observations made during the audit, and cumulative years of expertise, the overall findings demonstrate there's a continued lack of top management oversight and supervision of many entities' IT security functions. This is often referred to as the "tone at the top." Because an entity's IT security is ultimately the responsibility of top management, they have a duty to ensure that adequate safeguards are in place. These safeguards both protect the entity's data and limit the entities' risk to data exposure or loss.

Security Awareness Training Results

8 of 15 entities did not substantively comply with selected security awareness training controls we audited.

- Security awareness training programs inform staff and other users why security controls are necessary. Training programs also make staff aware where IT security risks come from. One of those risks is social engineering. Social engineering is when individuals try to manipulate, influence, or deceive people to circumvent internal controls and gain access to computer systems.

- We evaluated whether the entities complied with 5 controls related to security awareness and training. Those five controls, and our work to evaluate them, are described below. **Appendix C** also has more details on these five controls.

    - Security Awareness Policies: Entities should have documented security awareness training policies. We checked whether entities had a written policy requiring users to be trained and evaluated entities' security awareness training content.

    - Initial Training: Entities must provide security training to all new users within their first 90 days. We evaluated whether entities had trained new and existing staff in security awareness.

    - Annual Training: Entities must provide annual security training to all users annually.

- Mandatory Training Topics: Security training must include 12 specific training topics. For example, training must cover password security, physical security, and email and internet usage.

- Social Engineering: Entities must demonstrate their knowledge of security awareness training by passing social engineering tests. We conducted or reviewed email phishing campaigns at 11 entities. For the remaining 4 entity offices, we performed a walk-through to look for things like visible passwords, and confidential documents in accessible trash containers.

- For Security Awareness Training, 2 points are important to keep in mind:

  - We added 2 controls that are not in the state's security policy. The first includes an expectation that entities establish a security awareness training policy. The second involves testing users' understanding of security awareness.

  - The state's security policy requires all users to receive security awareness training. It defines users as any "employees, contractors, or other agents who act on behalf of the state or carry out state functions." This definition does not distinguish between individuals with or without access to computers.

- 8 of the 15 entities did not substantively comply with security awareness training controls we evaluated. **Figure 3** summarizes our findings in this area. As the figure shows, 6 entities had significant control issues and 2 had major control issues in this area. This means over half of the entities did not substantively comply (scoring 50% or less) in this area.

Figure 3. Eight of fifteen entities did not substantively comply with selected security awareness training controls.

Source: Summary of LPA analysis of selected IT security controls at 15 entities

Kansas Legislative Division of Post Audit

As shown in the figure, the other 7 entities had moderate control issues. None of the 15 entities had only minor issues (scoring above 75%). Our findings are summarized below.

- Security Awareness Policies: Most entities had weak or no policies requiring employees to take security awareness training. Having explicit, agency-specific policies signal to employees that security awareness training is important and supported by management.

- Initial Training: At each entity, we generally selected a random sample of 15-20 new employees to test whether they received initial security awareness training within the required 90 days. We found staff were not always trained timely or consistently. Our tests showed some entities did not train all sampled new staff or did not train all sampled staff for several months.

- Annual Training: At each entity, we selected a random sample of employees. For larger entities, that sample was 15-20 employees. At smaller entities, we tested the entire staff population. Our tests on annual training found entities did not always train all sampled employees. Some entities did not provide any security awareness training to its employees at all. Others exempted certain users (board members, student workers) from having to take the training despite ITEC requiring "all users" receive training. Although the results from these samples are not projectable, the issues we identified represented security threats. Their existence provided us reasonable assurance that problems existed.

- Mandatory Training Topics: Training programs did not always cover all 12 topics ITEC required. For example, programs sometimes lacked information on "software usage, copyrights, and file sharing." In other cases, information on passwords was incomplete.

- Social Engineering: At least one employee at 9 of the 11 tested entities clicked on simulated phishing emails. Click rates for these 9 entities ranged between 1% and 15%. Additionally, 3 of 4 entity offices failed our walk-throughs. We found trash cans with sensitive information at 1 entity, and an unlocked shred bin containing confidential material at another. In 1 instance, we saw login credentials (password) lying in plain sight.

- Security awareness training does not require sophisticated tools or expensive resources. Several entities made use of the security awareness training program available through KISO. Still, more than half of the entities performed poorly in this area, and none had sufficient controls to reach our "green zone" (above 75%).

- Security awareness training is important because people are the weakest link in an entity's security posture. Entities use technical hardware and software to put in place controls at many levels. But it only takes a small action by a single employee (e.g. clicking on a phishing link, not disposing of sensitive information properly) to bypass these technical controls.

- Based on interviews with auditees and our prior audit experience, the main reason for poor outcomes in this area is that top management didn't sufficiently prioritize compliance. Secondly, even when entities had training processes in place, leadership didn't sufficiently monitor them to ensure they worked as intended.

Account Security Results

10 of 15 entities did not substantively comply with selected account security controls we audited.

- Account security controls are designed to limit and track who has access to an entity's network and data. One example control is requiring passwords to be a specific length. Another control is to use multifactor authentication (MFA). MFA adds an extra step to the login process before a user can gain access to an account or application. This might be a one-time password sent to a phone or a physical fob or token. MFA provides a secondary safeguard in case the account password is compromised.

- We evaluated whether the entities complied with 5 controls related to account security. Those five controls, and our work to evaluate them, are described below. **Appendix C** has more details on these five controls.

    - Password Settings: There are two groups of accounts for which we evaluated controls related to password settings. One group was user accounts, and the other was service accounts. We reviewed entities' password settings to ensure they had sufficient length, and required a combination of letters, numbers, and special characters (complexity).

    - Lockout Settings: Accounts should be locked after 5 consecutive failed password attempts. We reviewed the entities' lockout settings to ensure they complied with this requirement.

    - Deactivated Accounts: Accounts of former employees must be deactivated or deleted in a timely manner. We checked whether IT staff at these entities did this and did it timely.

    - Multi-factor Authentication (MFA): Accounts with high-level permissions must use multi-factor authentication. We interviewed staff and evaluated accounts with high-level permissions to ensure MFA was required to access them.

- In this area, 2 points are important to keep in mind:

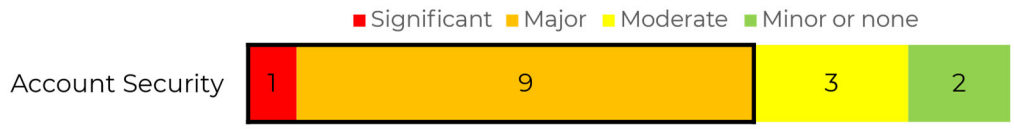
    - The state's security policy sets minimum requirements for account security. Entities may decide to enforce stronger controls for all users or

certain user groups with access to more sensitive data. When we saw multiple password settings, we checked whether they met the state's minimum requirements.

- Several entities failed multiple password settings. When that happens, hackers can try out numerous passwords until they find one that works. This is called "brute force attack." For example, an entity with a password setting allowing 8 characters, no complexity, and unlimited attempts (no lockout) is more vulnerable to brute force attacks.

- Most entities we reviewed (10 of 15) did not substantially comply with these account security controls. **Figure 4** summarizes our findings in this area. As the figure shows, 1 entity had significant control issues and 9 had major control issues in this area. This means over half of the entities did not substantively comply (scoring 50% or less) in this area.

Figure 4. Ten of fifteen entities did not substantively comply with selected account security controls.



Source: Summary of LPA analysis of selected IT security controls at 15 entities

Kansas Legislative Division of Post Audit

As shown in the figure, 3 entities had moderate control issues. The remaining 2 entities had minor findings. Our findings are summarized below.

- Password Settings: Passwords at 1 entity only had to be 4 characters long. Others had varying lengths that fell short of the required 12 characters.

- Lockout Settings: A few entities did not have a lockout configured. Several others' settings were weaker than required (e.g., up to 100 failed attempts vs. the required 5).

- Deactivated Accounts: We selected a random sample of employees that had departed during a period of time prior to the audit. For larger agencies, that sample was 15-20 employees. For smaller entities, we reviewed the account status of all employees that had left during the specified time period. We found accounts of former employees were not always deactivated for weeks or months after the person stopped working there. At some entities, we found some sampled accounts were not deactivated at all. Although the results from these samples are not

projectable, the issues we identified represented security threats. Their existence provided us reasonable assurance that problems existed.

  - Multi-factor Authentication: Most entities lacked multifactor authentication for accounts with higher levels of permissions.

- The controls we reviewed are relatively simple to enforce. In several smaller agencies, Office of Information Technology Services staff managed password settings for the auditee. Still, two-thirds of the entities performed poorly in this area, and only 2 had sufficient controls to reach our "green zone" (above 75%).

- When account security controls are weak or non-existent, it becomes easier for an unauthorized person to access or steal sensitive information or sabotage entity processes and infrastructure.

- Based on interviews with auditees and our prior audit experience, the main reason for poor outcomes in this area is inadequate management oversight (IT and non-IT) to ensure account security controls were followed. Second, several entities had limited IT staff, lacked IT security expertise, or both. Staffing and skills deficits suggest that top management is not sufficiently prioritizing IT security. We also noted multiple entities where non-IT staff did not appear to appreciate the importance of certain IT controls.

Incident Response Results

8 of 15 entities did not substantively comply with selected incident response controls we audited.

- Incident response plans document entities' steps to detect, isolate, contain, and fix a security incident. Security incidents can vary widely in scope and seriousness. They can be small (accidentally sending non-public personal information to the wrong person). They can be large (network breach or ransomware attack). Incident response processes should include a definition of security incident. Testing the plan ensures that it works the way it's supposed to.

- We selected 5 incident response controls from the state's security policy to evaluate. Those five controls, and our work to evaluate them, are described below. **Appendix C** has more information on these 5 controls.

  - Incident Response Plan: Entities must have a documented incident response plan. We checked whether entities had these plans, and that they included required sections such as planning, detection, and containment.

  - Defined Security Incident: Entities must define and document what constitutes a security incident. We checked whether the entities had a

definition of a security incident (this must include intentional and unintentional incidents).

- Incident Response Testing: Entities must test or otherwise use their incident response plans each year. We interviewed staff and reviewed entities' incident response testing documentation.

- Incident Tracking and Categorization: Entities must have a process to track and categorize the severity of security incidents. We interviewed staff and reviewed documents to determine whether entities had a process to track and categorize incidents.

- Post-Incident Response: Entities must review their response to significant incidents and communicate the information to leadership. We reviewed entities' post-incident processes.

- In this area, 2 points are important to keep in mind:

  - 5 entities created their incident response plan during our audit. We accepted those plans if they were finalized and not in draft form. We deducted points only when those plans had significant issues.

  - Some entities told us they did not have an incident response plan. Those entities did not get any points on that item. Because they did not have a plan, we also did not evaluate the plan's testing.

- 8 of the 15 entities did not substantially comply with the incident response controls we reviewed. **Figure 5** summarizes our findings in this area. As the figure shows, 6 entities had significant control issues and 2 had major control issues in this area. This means over half of the entities did not substantively comply (scoring 50% or less) in this area.

Figure 5. Eight of fifteen entities did not substantively comply with selected incident response controls.

Source: Summary of LPA analysis of selected IT security controls at 15 entities

As shown in the figure, 4 entities had moderate control issues, and the remaining 3 entities had minor or no control issues. Below is a summary of our findings.

- Incident Response Plan: Some entities lacked an incident response plan. At 1 entity, staff suggested that staff turnover and shortages had prevented them from putting a plan together.

- Defined Security Incident: Some entities did not define security incident in their incident response plans or other policies. Others' definitions did not clarify that unintentional actions could qualify as incidents.

- Incident Response Testing: Entities who had incident response plans prior to our audit tested or used them in 2022. We saw documentation to support this.

- Incident Tracking and Categorization: Some entities did not have processes to track or categorize the severity of the incidents. At 1 entity, staff said they rated all incidents as "high." This could lead to resource issues if more than 1 incident occurs at the same time.

- Post-Incident Response: Many entities had weak post-incident processes or those processes were not documented. For example, at 1 entity, staff told us about significant security incidents that had occurred in the previous 3 years. Staff told us post-incident reviews had taken place, but the reviews were not documented.

- Incident response controls have been part of the state's security policy and other standards for a long time. With the increase of cybersecurity attacks such as ransomware and data breaches, it is imperative entities have a game plan for when a security incident is suspected. A myriad of templates and resources exist from entities such as KISO, NIST, CIS, and K12 Security Information Exchange (a national non-profit organization dedicated to protect the K-12 community). Still, more than half of the entities did not substantively comply (scoring 50% or less) in this area. And only 2 had sufficient controls to reach our "green zone" (higher than 75%).

- Having adequate incident response controls increases the chance of successfully handling security incidents. Non-technical staff may not know to notify IT staff about suspicious events if entities haven't defined what a security incident is. Entities won't know whether their incident response plans will work like they're supposed to unless they test them. Testing provides a safe, controlled environment to identify those issues.

- Based on our work and prior audit experience, several reasons exist for poor results in this area. First, incident response planning is a form of strategic planning. Strategic planning may be a luxury that IT staff don't have time for when "putting out fires." Secondly, IT staff at multiple entities appeared

understaffed, which can lead to strategic planning being put on the back burner. We also learned that IT staff sometimes believe they can adequately deal with situations as they arise. They don't appear to appreciate the value of documented processes. Lastly, top management may view incident response as an IT responsibility they have nothing to do with. Similarly, they may not understand why incident response planning and documentation is important.

Other Findings

Enrolled House Bill 2019 relies on an organizational structure in which audits may not be conducted objectively or independently.

- The law requires the Kansas Information Security Office (KISO), under direction of the state's Chief Information Security Officer (CISO), to perform audits of executive-branch agencies. Those audits should cover applicable state and federal laws, rules and regulations, executive branch policies and standards, as well as ITEC policies.

- This structure creates independence issues. The Government Auditing Standards ("Yellow Book") published by the United States Government Accountability Office includes key concepts for conducting high quality audits. Those concepts are integrity, objectivity, and independence. The Yellow Book describes various types of independence threats, including self-review, bias, undue influence, and management participation.

- KISO staff advise – and at times work for – executive branch agencies. K.S.A. 75-7238 requires the CISO to coordinate cybersecurity efforts between executive branch agencies. It also requires the CISO to provide guidance on potential security incidents. Therefore, KISO staff, under the direction of the CISO, would end up auditing some of their own work or performance. This can create bias, independence, and objectivity issues.

- Governmental audits do not have to follow Yellow Book standards. The Yellow Book also allows auditors to continue audits despite independence issues. In those cases, the report must clearly state that the audit was NOT conducted under Yellow Book Standards, or include proper disclosures and caveats. However, when government audits do not comply with independence or other key requirements, their overall value may be diminished.

Conclusion

Nearly 10 years ago, we recommended the legislature create a more enterprise-level approach to IT security to help improve agencies' security posture. The legislature responded by creating the Cybersecurity Act in 2018. This included the new Kansas

Information Security Office and a state Chief Information Security Officer position. The 2023 legislature further strengthened the Cybersecurity Act. ITEC also approved several updates to its policies, including the statewide IT security policy, in recent years.

Despite these improvements, we continue to identify weaknesses with state agencies' basic security controls. In this audit, we selected several smaller state agencies as well as larger ones. While smaller agencies may not hold the most sensitive confidential data, the audit shows they have similar compliance problems as their larger counterparts.

The Cybersecurity Act explicitly made agency heads responsible for their agencies' security compliance. Given the findings in this audit, we continue to think that agency leaders don't know or sufficiently prioritize their IT security responsibilities. Agency leaders also may not sufficiently monitor whether their staff implement controls adequately. This could be because the Act does not include consequences for noncompliance. Additionally, the state currently doesn't have a centralized solution to ensure agency heads are made aware of those responsibilities in a consistent manner. KISO may be the most logical entity to do this for most agencies, but they may not be in the best position to educate elected or non-executive state agencies.

Other factors contributed to the audit's findings. The shortage of IT security experts appears to be worsening. It can be challenging to compete with the private sector to find knowledgeable IT staff. Still, many of the controls evaluated in this audit do not require special IT security knowledge or expensive resources. Agencies can also ask for help from the Kansas Information Security Office if needed.

School districts may be further behind in building strong security processes. That's because they are still not required to adopt basic security standards. Despite the actions KSDE has taken, it's unlikely that smaller districts with fewer resources will adopt security standards. In turn, larger districts are better positioned to adopt and implement security controls, when given the choice.

Recommendations

1. All 15 entities we audited should review the individual control findings they received during the audit. They should determine what actions they can take to remedy the findings and how to prioritize them, in light of their overall risk appetite. As needed, entities could reach out to KISO, KSDE, or K12 SIX for assistance or advice.

- Office of the State Bank Commissioner Response: Based on the LPA's findings, our agency created a remediation plan and has already begun to address the minor deficiencies discovered.
- Behavioral Sciences Regulatory Board Response: We appreciate the review and feedback from the members of the Legislative Division of Post Audit. In general, we were pleased to have received mostly positive marks in different areas, though we appreciated the highlighted areas of improvement. Since the audit, we have prioritized items for improvements and we have held multiple meetings with representatives from the groups that assist us with services, to make immediate changes and to build better policies for the future.
- Board of Cosmetology Response: We have taken into consideration each of the findings observed during the 2023 LPA and are taking the appropriate steps to implement and act on each of the recommendations.
- Board of Tax Appeals Response: The agency has implemented policies and procedures and is weighing options to remediate all reported findings.
- Commission on Veterans' Affairs Response: We intend to implement policy and procedural changes that follows the guidance from ITEC policy 7230A and recommendations from KISO regarding information security awareness. We also intend to implement control measures like multifactor authentication where appropriate.
- Department of Administration Response: The agency recognizes the audit findings and will determine a best path forward toward addressing the identified exceptions.
- Department of Wildlife and Parks Response: The agency has received the summary and individual findings and recommendations reports from the Legislative Post Audit. In reviewing the reports, KDWP has implemented changes to businesses processes to remedy immediate recommendations. The agency has also put into the agency project schedule to implement recommendations that will take a longer term to incorporate.
- Fort Hays State University Response: Fort Hays State University appreciates the time and effort of Kansas Legislative Division of Post Audit for performing the audit and providing their findings to us. After an initial review of the findings, we believe the information provided is generally accurate and can be useful in improving our overall security posture. We have already implemented several fixes to address some of the issues that were found. At this time, we are continuing to review the findings and examining our systems and policies to determine what else we can do to mitigate remaining issues and reduce our overall risk.
- Kansas Highway Patrol Response: We have reviewed the LPA's 2023 IT Security Summary Report and are in the process of taking steps to remedy each area of concern. Concerns relating to Security Awareness Training, Account Security and Incident Response are being addressed, and meetings

are currently underway to ensure that the LPA's findings are properly addressed, as applicable.

- Kansas Human Rights Commission Response: The agency has implemented LPA recommendation number 1. We have reviewed the individual control findings, determined what actions can be taken to remedy any findings and how to prioritize them, if any findings were recommended for a remedy. Internal control findings for our agency have been forwarded to a representative with the Kansas Information Security Office (KISO) for agency coordination with KISO.
- Kansas School for Blind and School for Deaf Joint Response: We recognize that we have significant security risks and intend to investigate and resolve all issues identified in the report to the best of our ability while ensuring that the resolutions impact our students' ability to learn and access resources to the least extent possible. Up to this point, we have not had guidance or resources to assist in identifying and resolving these issues and are excited to work with the above-named entities to resolve these short-comings to the best of our ability. One of the major issues cited time and again in the report was staffing and we agree with this finding, with the limited resources available, it has been almost impossible to attain and retain the personnel needed to meet these standards.
- Lansing School District (USD 469) Response: We are reviewing each finding and assessing what needs to be done to address each issue. We have begun addressing critical issues and gathering examples of policy items that need to be updated. We have developed a project board in response to track our progress in addressing each finding.
- Bonner Springs School District (USD 204) Response: We have reviewed the individual control findings provided and plan on making changes based on those recommendations to us, within our means. This will help us plan for future improvements and prioritize areas that are needed.
- Hutchinson School District (USD 308) Response: USD 308 will implement the recommendation.

2. All 15 entities should report their progress to us by December 1, 2023 as part of our 6-month follow up process, taking a clear position on which findings are fixed, in progress, not started, or refused.
    - Office of the State Bank Commissioner Response: Our agency looks forward to our six-month follow-up and are confident in our ability to remedy the identified findings.
    - Behavioral Sciences Regulatory Board Response: We are happy to comply with the direction from the member of the Legislative Division of Post Audit. While we were asked to report progress by December 1, 2023, we wanted to share with the members of the Legislature that immediately following the fieldwork from the members of LPA, we took action to modify language in our Security Incident Response Plan clear up any vagueness or ambiguity and to

add specific terms requested by representatives of LPA. We realize that these immediate corrections did not change our score in the report from LPA, but we wanted to demonstrate that we were proactive in addressing issues as soon as they were brought to light. Additionally, we have met with our own staff to enforce good practices and to encourage staff members to be even more diligent concerning risks, such as phishing attempts. We are happy to continue to focus on positive improvements and we will provide good information to LPA by December 1, 2023, showing a clear position on which findings are fixed, in progress, not started, or refused.

- Board of Cosmetology Response: Our agency plans to report progress by December 1, 2023.
- Board of Tax Appeals Response: The agency will submit an updated report by December 1, 2023 reporting progress on the findings and actions listed above.
- Commission on Veterans' Affairs Response: We will report progress to the LPA by December 1, 2023. We will be updating policy relating to Security Awareness Training. We have already implemented specific changes to include online security awareness training via the KLPM portal. This ensures that all 12 areas of security awareness will be covered. Our Agency will implement updates for password security recommendations. Furthermore, we will be evaluating incident response plans to make necessary changes to ensure compliance. We will continue to update and implement policies and procedures designed to increase cyber security overall.
- Department of Administration Response: The agency will provide the LPA with a progress update as requested by December 1, 2023.
- Department of Wildlife and Parks Response: The agency recognizes the 6-month follow up process of the Legislative Post Audit (LPA) and will work with the LPA come December to report progress on the recommendations.
- Fort Hays State University Response: Yes, Fort Hays State University plans to report our progress on fixing issues identified in the LPA Audit report by Dec. 1, 2023.
- Kansas Highway Patrol Response: We will report our progress to the Legislative Post Audit by December 1, 2023, as we intend to remedy all of the concerns as applicable relating to Security Awareness Training, Account Security and Incident Response by that time.
- Kansas Human Rights Commission Response: The agency will implement LPA recommendation number 2 by reporting the agency's progress to LPA on or before December 1, 2023 as part of LPA's six-month follow up process, with intentions to take a clear position on which findings are fixed, in progress, not started or refused, if any findings were recommended for a remedy. We will be working with a representative from the Kansas Information Security Office on this LPA recommendation.
- Kansas School for Blind and School for Deaf Joint Response: We will start working on all findings to the best of our ability. Any assistance that can be

provided would be greatly appreciated. We will mark our calendars for Dec. 1 and intend to have made progress on the majority of findings.

- USD 469 Lansing Response: We intend to report our progress to the LPA group by December 1, 2023. Our response will include documentation of policies and procedures as well as a checklist of items addressed on our project board.
- Bonner Springs School District (USD 204) Response: This Agency will report back on its progress by December 1, 2023 explaining the progress and solutions we have taken based on the recommendations report.
- Hutchinson School District (USD 308) Response: USD 308 will implement the recommendation.

3. KSDE should require all school districts to adopt basic security standards based on current industry standards. Given funding and local control issues, those standards could include an exemption section to allow districts to identify controls they cannot yet meet.
    - Department of Education Response: The Kansas State Board of Education adopted four strategic, targeted goals at its May 2023 board meeting. The goals and related outcomes are the result of the Board's retreat sessions in February and March. One of the four goals is to "enhance the safety and security of school districts in Kansas." The desired outcome is to diminish the threat and severity of school violence and cybersecurity attacks on school districts. KSDE has no legal authority to require school districts to adopt basic security standards, however the agency has recommended districts follow ITEC standards and has made those standards available on the KSDE website for school districts use.

4. To help districts fix missing controls, KSDE should help connect districts with necessary resources or grants, encourage collaboration among districts, and request authorization for additional agency staff to provide such assistance.
    - Department of Education Response: The Information Technology (IT) team at KSDE was established and staffed to meet the data collection and management needs of the Department, rather than school districts. The level of support necessary to implement this recommendation would be a significant undertaking and is not possible with the current level of IT staffing at KSDE. KSDE provides school district technology directors with information and possible resources to address questions as they arise. As the LPA recommendation states, providing additional support would require additional staff and resources. Combined with the first recommendation, the number of staff and amount of resources will depend on the level of support required by future statute. As an example, Kentucky has a staff of 41 specifically to provide IT support for school districts.

5. The legislature should consider amending the Cybersecurity Act to require KISO to educate all new and current agency leaders annually about their responsibilities regarding information security. This may be part of the statutorily required leadership training program or take other forms. Ideally, it should include a deliverable that agency leaders receive to remind them of key information.

6. The legislature should consider revising the Cybersecurity Act to reduce or eliminate the potential independence and objectivity issues related to KISO's new audit requirements identified in the Other Findings section.

Agency Responses

On Monday, May 30, 2023 we provided the draft audit report to the 15 audited entities listed in **Appendix A** as well as the Kansas Department of Education. Although all of the entities responded to the recommendations, some chose not to provide a general response. The Department of Education rejected our recommendations and chose not to submit a general response. Responses from entities that chose to respond are listed below. Entity officials generally agreed with our findings and conclusions. However, officials from Behavioral Sciences Regulatory Board disagreed with some individual findings related to incident response and security awareness. We reviewed the information officials provided and made minor changes to our findings in the incident response area.

Behavioral Sciences Regulatory Board Response

General Response to LPA Audit

We appreciate the review and feedback from the members of the Legislative Division of Post Audit. We value the importance of securing information and having good policies, practices, and technology to safeguard that information. We appreciate the comments that noted areas of improvement and we are happy to comply with the direction from the member of the Legislative Division of Post Audit.

While we look forward to continuing to work with members of LPA as we improve our processes, we wanted to share a few items of concern, regarding this particular audit:

1. In general, the feedback we received from members of the Legislative Post Audit were positive, however as this is an audit that groups several different agencies/entities, we are concerned that problems identified with other agencies/entities will be inferred on all audited groups. Additionally, we are concerned that generalized comments regarding the possible causes of these problems will be inferred on all audited groups, regardless of whether that was true for each of those agencies/entities.

2. In reviewing the findings of LPA, we noted that at times, the standards applied to agencies/entities were ITEC standards, while at other times the standards being scored were not ITEC standards, but rather higher “best practices” standards. In one example, it was found that we met the standard in the ITEC policy to require all users to complete security awareness training with ninety (90) days of hire or initial access and to retain a form of acknowledgement of training completion and it was found that we required all employees to complete the training and had documentation showing this completion, however we were cited as having a problem in the audit, and a corresponding lower score, as we did not meet the “best practices” standard that was applied to have an agency-specific written policy that stated it was an

agency requirement to complete those annual security awareness trainings. It would be helpful for future agencies/entities to have consistent standards for being evaluated.

LPA Note: The two standards referred to were evaluated and scored separately. The agency received credit for training staff (an ITEC requirement), but did not receive credit for not having a related policy (a best practice).

Board of Cosmetology Response

Our agency leadership and staff understand the importance of protecting the sensitive data we collect. We have implemented strict IT security policies that adhere to ITEC 7230A.

Board of Tax Appeals Response

Response to the Kansas Division of Post Audit Report
"Information Systems: Reviewing Specific IT Security Controls Across State Agencies and School Districts, July 2023"

The Kansas Board of Tax Appeals appreciated the opportunity to participate in this year's audit and extends a well-deserved thank you to the Kansas Division of Post Audit's staff and our colleagues at the Kansas Information Security Office. The audit provided an ideal platform to review critical information security controls and identify any gaps in compliance, which has allowed the Agency to focus and refine its pursuits in information security. Over the last few years, the Agency has had its fair share of challenges, particularly with respect to information technology support, and staffing. The Agency hired an information technology manager in August of 2022 to rebuild its information technology program and spearhead a coordinated program to modernize its technology infrastructure, including efforts to address critical security concerns. The audit provided the Agency a timely opportunity to review its internal policies and procedures as well as its IT modernization program to ensure compliance with state requirements. We look forward to further collaboration with KISO and again thank the Division of Post Audit for the opportunity to provide a response and commentary for this year's audit.

Bonner Springs School District (USD 204) Response

We have discussed and looked over all the information provided by us from the audit team. We will be looking at this as an opportunity to reflect on what we have fallen short on and how we can correct and improve on the areas given. Thank you.

Appendix A – Cited References

This appendix lists the major publications we relied on for this report.

- Information Technology Security Standards 7230A (July 2019). *Kansas Information Technology Executive Council*.

- CIS Critical Security Controls Version 8 (May 2021). *Center for Internet Security*.

- NIST Special Publication 800-50-Building an Information Technology Security Awareness and Training Program (October 2003). *National Institute of Standards and Technology*.

- School Districts' Self-Reported IT Security Practices and Resources (October 2021). *Kansas Legislative Division of Post Audit*.

- State Agency Information Systems: Reviewing Security Controls in Selected State agencies (CY 2014-2016) (December 2016). *Kansas Legislative Division of Post Audit*.

- 3 Year Summary of Security Controls in Selected State Agencies (2017-2019) (February 2020). *Kansas Legislative Division of Post Audit*.

- 3 Year Summary of Security Controls in Selected State Agencies (2020-2022) (December 2022). *Kansas Legislative Division of Post Audit*.

Appendix B – List of Audited Entities

This appendix lists the 15 entities we selected for audit. The list includes each entity's expenditures and FTE.

Agency Name		2022 Expenditures	2022 FTE
Department of Administration	$	1,113,305,101	467.7
Fort Hays State University	$	172,285,759	1,013.5
Kansas Highway Patrol	$	97,127,404	880.0
Department of Wildlife and Parks	$	94,899,040	453.0
Hutchinson School District (USD 308)	$	78,185,187	882.1
Bonner Springs School District (USD 204)	$	40,576,727	418.3
Lansing School District (USD 469)	$	37,571,538	371.5
Commission on Veterans Affairs Office	$	27,002,805	373.0
Office of the State Bank Commissioner	$	12,713,048	110.0
School for the Deaf	$	12,324,706	143.5
School for the Blind	$	8,189,390	81.5
Board of Tax Appeals	$	1,710,672	16.0
Kansas Human Rights Commission	$	1,333,397	23.0
Board of Cosmetology	$	1,198,151	14.0
Behavioral Sciences Regulatory Board	$	1,073,817	9.5

Source: FY 2024 Governor's Budget Report Vol. 2, and Kansas Dept. of Education Data Warehouse, school year 2021-22 (unaudited).

Appendix C – List of Selected Security Controls by Area

This appendix includes the selected controls across the 3 security areas we selected for audit. The list includes the source of each control.

	Area 1 – Security Awareness Controls	Source
1	Entities must have documented policies on Security Awareness Training.	NIST 800-50
2	Entities must require all users to complete security awareness training within ninety (90) days of hire or initial access. Entities must retain a form of acknowledgement of training completion.	ITEC 8.2, 8.3
3	Entities must require all users to complete security awareness training on an annual basis. Entities must retain a form of acknowledgement of training completion. [In Section 5.16, Users are defined as employees, contractors, or other agents acting on behalf of the state or carrying out state agency functions.]	ITEC 8.1 - 8.3
4	Awareness training must address the following topics at a minimum: • Passwords including creation, changing, aging, and confidentiality • Privacy and proper handling of sensitive information • Physical security • Social engineering • Identity theft avoidance and action • Email usage • Internet usage • Viruses and malware • Software usage, copyrights, and file sharing • Portable electronic devices and portable electronic media • Proper use of encryption devices • Reporting of suspicious activity and abuse	ITEC 8.5
5	Entity staff must demonstrate their SAT understanding by passing social engineering tests (phishing and/or physical environment)	CIS 14.2

Source: LPA review of ITEC 7230A, NIST 800-50, and CIS 14.2.

	Area 2 – Account Security Controls	Source
1	Information System accounts must be restricted to a maximum of five (5) consecutive failed attempts before being locked. Accounts must remain locked for a minimum of thirty (30) minutes without administrator intervention.	ITEC 9.17, 9.18

2	Passwords for system user accounts must be constructed with the following requirements:
	• A minimum of twelve (12) characters in length, contain three (3) of four (4) of the following categories:
	  ○ Uppercase
	  ○ Lowercase
	  ○ Numeral
	  ○ Non-alpha numeric character
	• Must not contain the user ID
	• Must not have a lifespan that exceeds 180 days
		ITEC 9.11.1 - 9.11.3 9.11.5

3	Passwords for system service accounts must be constructed with the following requirements:
	• A minimum of twelve (12) characters in length.
	• Contain three (3) of four (4) of the following categories:
	  ○ Uppercase
	  ○ Lowercase
	  ○ Numeral
	  ○ Non-alpha numeric characters
	• Must not contain the user ID.
	• Passwords for system service accounts must not have a lifespan that exceeds three hundred sixty-five (365) days.
		ITEC 9.12.1-9.12.4

4	Entities must revoke system access or eliminate unnecessary permissions for user accounts as users are transferred, terminated, or their role has changed.	ITEC 17.8
5	Multi-factor authentication must be used for administrative rights or elevated privilege accounts.	ITEC 9.3.2

Source: LPA review of ITEC 7230A.

	Area 3 – Incident Response Controls	Source
1	Entities must adopt a documented incident response plan which addresses the following stages: preparing for a security incident, detecting and analyzing a security incident; containing a security incident; eradicating and recovering from a security incident; and post incident activities.	ITEC 15.1
2	Entities must define and document what constitutes a security incident. Security incidents must include intentional and unintentional incidents.	ITEC 15.2
3	Entities must annually conduct IR operations testing using classroom, tabletop exercises, or live incidents.	ITEC 15.7
4	Entities must define and document a process to track and categorize the severity of all incidents which must drive the associated response, reporting and communication activities.	ITEC 15.3
5	For significant security incidents, entities must perform a post incident review within a reasonable timeframe upon containment. Post incident review documentation must be communicated to entity leadership.	ITEC 15.11

Source: LPA review of ITEC 7230A.