Mr. Chair and members of the Committee!

Before I start going over the specific IT security findings for a couple of agencies to demonstrate what types of IT security problems we are finding, I want to take just a few minutes to provide some context—where our IT security audit function came from, and where we are going, starting with the audits you hear today.

Legislative Post Audit has conducted IT security audits for more than 12 years. Over that time, the process has evolved quite a bit.

- In the beginning, we limited our audits to one agency, and focused on a few areas within the broader spectrum of IT security, such as
    - server and workstation patching processes,
    - plans for continuing operations in the event of emergencies, and
    - change control
- Since then, we have expanded coverage in both the number of agencies and the number of security areas audited.

Our **CURRENT triennial plan** began in 2014 and finishes this December (2016).

- As part of that plan, we first conducted an audit which gathered information statewide about the types, volume and variety of sensitive data agencies have. This was presented in July 2014. (R-14-007)
- Using information from that audit, we put together a risk-based process that we used to select agencies for in-depth IT security audits. I will present highlights from two of these audits shortly.

I'd like to cover **HOW OUR WORK HAS CHANGED**, partly based on feedback from the audited agencies, and partly because our audit function and personnel has grown in sophistication:

- First, I'm proud to point out our team is highly credentialed. Members of our team hold at least one certification, such as the CISA (Certified Information Systems Auditor), and some require extensive technical knowledge (like the CISSP).

- Second, we have streamlined our work to cover more ground in less time.

- As I mentioned earlier, in years past we concentrated our work on certain IT security areas (8 in 2013), our latest round of audits covered 20 IT security areas.
    - Within these main areas, we evaluate whether agencies adhere to specific requirements set out by the Kansas Information Technology Executive Council (or ITEC).
    - We also evaluate agencies' adherence to best practices we think are important, but are not part of the statewide ITEC requirements.

- Altogether, we now evaluate about 100 different requirements across these 20 areas FOR EACH AGENCY, which is important to keep in mind when I summarize the findings from the individual agencies.
- We evaluate many of these requirements at the agency-wide level. Additionally, we also evaluate some specific IT security controls for ONE of the agency's system applications that holds sensitive information.

- Lastly, I want to quickly explain how we move through these audits:
    - In the first phase, the agency completes a **self-assessment** to document whether THEY believe they comply with the requirements.
    - In the second phase, we hold an **in-depth interview** so we can learn about the agency's IT function and ask follow up questions to the completed self-assessment.
        - We also allow agencies to opt into social engineering testing.
            - In 2015, we began offering audited agencies this optional service.
            - Agencies agree to overall rules of engagement, but are otherwise not warned of which techniques will be used or when.
    - In the third phase, we **go onsite** and conduct fieldwork.
        - We review training files for employees, view computer screenshots, and review policies and procedures and other documentation to determine whether the agency complies with ITEC requirements and best practices.

        - During this phase, we also run a scan of the agency's workstations and servers which tells us whether the agency has adequately patched its computers to protect against known vulnerabilities.
    - After our week-long onsite visit, we document, discuss and **synthesize the findings**, with the occasional follow up with the agencies.
    - We then **evaluate the level of severity** we think the problem presents. A critical risk finding is a vulnerability that creates an imminent threat for data loss. On the other side of the spectrum, technical findings are weaknesses in the agency's documentation or security process that are unlikely to lead to present or future vulnerabilities.
    - Last, we communicate our preliminary findings to the agency at an **exit conference**.

I present this to explain efforts in streamlining and working with the agencies to create the least interruption, as that has been a concern they brought to us.

That concludes the public portion of my presentation. Once in executive session, I will continue with the results of two of our IT security audit reports. Otherwise, I'd be happy to stand for questions.