Mr. Chairman, Members of the Committee:

My name is Rob Arnold. I have served as Information Security Officer at the University of Kansas for the past two years. Prior to that I worked for seventeen years in financial services. I have been a practitioner of information security for seventeen years, and have eight years' experience leading information security teams and being responsible for security programs. I hold the professional designations Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

I would like to thank the committee for the opportunity to address you today. I will address questions related to the recommendations found in Legislative Post Audit report R-14-007, *State Agency Information Systems: Sensitive Datasets and IT Security Resources*. Three themes were raised for legislative consideration in the conclusions of the report: structural issues affecting delivery of security functions, the role of the private sector, and staffing the security function.

Structure enables success

To speak directly to the question of effectiveness, "are the state's IT Security resources adequate to meet the current need?" involves special attention to the structures that support good security outcomes. The Council on CyberSecurity identifies a short list of suggestions in its *Cybersecurity Workforce Handbook*: clear accountability, establish a response team, measure and report, invest in training and development, build external relationships, develop career pathways, establish mentorship, and build the brand.

From my experience leading information security programs, I would prioritize the first three suggestions from this list. Establishing the accountability and defining measures of success creates structure that enables the success of a security program. This makes accountability a critical success factor in any enterprise security plan.

KU's security program benefits from clear accountability. The Information Security Office derives authority and scope of duties from policy. The policy also articulates responsibilities for IT staff, for authorized users of IT, and for a computer security incident response team (CSIRT). The inclusion of the CSIRT in policy reflects the priority and importance assigned to the response function at KU.

A strong focus on reporting allows me to assert that KU's incident response time for security incidents during calendar year 2014 places us in the top 10% of all organizations with this capability. This benchmark comes from the *2013 Verizon Data Breach Investigation Report*. The Verizon report also points out that 66% of breaches remain undiscovered by organizations for months or more, which helps underscore the importance of a strong response capability.

Having an effective response team is the top operational priority within the capabilities of a modern enterprise security team. Reliance on prevention has proved ineffective, so emphasis on robust response is the current best practice. The structure in KU's security program, defining my role as accountable and providing clear reporting lines, enables the operational success of our incident response function. So these three priorities (two structural and one operational) are foundational elements of KU's information security program.

Private sector role

A more difficult question is "how and to what extent can the private sector assist in meeting the state's security goals?" The market for managed security services is currently a $15 Billion global market, projected to grow to $33 Billion by 2020. The private sector is a crucial part of this demand as well as the supply. Opportunities to augment the state's capabilities using managed security service providers exist, but careful vendor management will be a critical success factor.

Planning for a mixed source model with the ability to loosely couple with different vendors will enable a quicker time to value on future security projects if the state chooses that option. But the merger and acquisition activity in the security provider space is intense, which poses a degree of risk and highlights the need for vendor management.

Making sure the enterprise security plan for Kansas both embraces mixed sourcing and mitigates the risks of reliance on outside entities for critical security services will be a careful balancing act. My experience suggests judiciously applying mixed sourcing to tactical projects with short turn times to get quick results on security services that are more transactional and less strategic, or where economies of scale apply. Reserving internal capacity to take on transformational work is one compelling reason to use mixed sourcing.

Private sector involvement will require tradeoffs, as security decisions always do. Some types of security work can be traded off for money and vendor management work. Managed security services work best when the performance of work can be easily governed by a service level agreement.

Staffing the security function

To give some context to the findings in the audit report that relate to staffing, the concerns raised, while significant, are more reflective of the employment environment than they are of the state's approach to staffing the security function. The report highlights a specific risk that arises when lead security positions go unfilled for a long time.

This risk affects the public and private sector. A 2014 study of 504 organizations by the Ponemon Institute examined this staffing issue and found that 36% of security positions and 58% of senior security positions went unfilled in 2013. 70% of those organizations responded that their security function is understaffed. The top reason listed for why positions go unfilled was inability to offer a competitive salary, with 43% of respondents choosing it. 5.1 months to fill a security position, and 9.2 months for a senior security position are average according to this current research.

A 2014 BurningGlass report points out a 74% growth in security job postings for the time period 2007-2013, and finds that security jobs take 24% longer to fill than all IT jobs, and 36% longer to fill than all jobs. This report also finds that in 2013 U. S. employers posted 50,000 jobs requiring the information security credential CISSP, recruiting from a pool of only 60,000 CISSP holders. The clear conclusion is that demand is outstripping supply for highly qualified security talent.

Numbers from the Bureau of Labor Statistics reinforce the point and provide local insight. The most recent Occupational Employment Statistics report (May 2013) lists 70 information security analyst positions in the Topeka metropolitan area. That small talent pool it is indicative of the problem with trying to recruit qualified security professionals locally. Median wage is listed as $68,330, which is just higher than the 25th percentile nationwide figure of $67,120. So salary pressure from the east and west coast is also draining the Kansas talent pool of qualified information security staff.

The talent market for qualified security professionals also constrains the capacity of the managed services sector to provide services in this area. Security providers in this area are nearly always hiring qualified staff, posing additional retention challenges for state agencies. The security strategy includes staff development plans with the goals of retaining security talent and developing new security staff. One compelling advantage we have at KU is being able to recruit students to the security field in several ways. We employ them directly in the security office, and we guest lecture in classes related to information security, emphasizing the employment market and the need for qualified security staff.

A robust security plan for Kansas needs to address the security staffing challenge from the supply side as well as demand.

Summary:

Thinking about how to solve security problems at the scale of state government will require diligent attention to the fundamentals of information security management. Certain key issues are constraining the capacity of state agencies to accomplish their security goals. These key issues are well highlighted in the report from Legislative Division of Post Audit, *State Agency Information Systems: Sensitive Datasets and IT Security Resources.*

Thoughtful engagement from leadership as exemplified in the interest of the committee members today is critical to success. The private sector shows evidence of increasing engagement, with information security discussions a prominent feature in board rooms. Many more questions than the few I could explore today will need to be examined in the course of building the state's direction.

Engaged leadership that focuses on a "short list" of security priorities will allow the state to move purposefully toward the security posture it wants to have. The landscape of security is complicated, so "doing less but doing it better" is a strategy to build some momentum towards the state's security goals.

Thank you for your attention and consideration. I will be pleased to respond to questions at the appropriate time.