Office of Information Technology Services
2800 SW Topeka Blvd.
Topeka, KS 66611 (785) 296-7440

Testimony of the Chief Information Security Officer
Use of Cybersecurity Appropriation and State of Cybersecurity in Executive Branch Agencies
Before the Joint Committee on Information Technology (JCIT)
September 22nd, 2017

Mr. Chairman and members of the committee, I am Joe Acosta Chief Information Security Officer for the Executive Branch. Thank you for allowing me this opportunity to speak today and respond to questions and comments posed in the previous session. I would like to respond to Representative Esau's question regarding the potential impact the Jim Morrison Cybersecurity Bill may have on state cybersecurity efforts, and answer Representative Curtis' question regarding a roll out plan for small agencies.

In previous testimony, it was explained why providing an accurate assessment of cybersecurity in state agencies is challenging. Today I would like to briefly revisit that testimony, and provide some generally accepted professional observations of security in state government by myself and colleagues in other states. While it is true that we are unable to provide specifics about individual agencies, I would like to offer the common challenges that all State CISOs encounter in decentralized environments as we currently have in Kansas.

First and foremost is that there is roughly a 30% global shortage of qualified cybersecurity professionals with whom both private and public sectors compete. Here in Kansas the shortage is by far more extreme and our most significant challenge. Because of this shortage, we are unable to perform the most basic of cybersecurity functions, current agency efforts are superficial at best. Across the country, State CISOs are attempting to pry cybersecurity functions from general technologists, but this has proven to be challenging in environments where the State CISO has no authority. By leaving these tasks to unqualified staff, organizations are left extremely vulnerable and their data is at a high risk of compromise.

Complicating the shortage further is a misunderstanding that cybersecurity is something that can be solved by implementation of technology, this is inaccurate. While technology certainly has its role, cybersecurity also includes people and process. To address people and process a cybersecurity professional specializing in assurance must be available to assess, assist and report risk directly to the senior leadership of the organization. Knowing that we are not likely to find adequate numbers of staff for all agencies it only makes sense that we consolidate and share the resources that we have. Our current FY18 and FY19 budgets do not afford the KISO office the ability to hire security professionals for the enterprise.

This speaks directly to Representative Esau's question last session of how would the Jim Morrison Cybersecurity Act impact the state of cybersecurity in Kansas. I would offer that the proposed authorities and responsibilities of the CISO and the centralization of cybersecurity in the bill are exactly what's necessary for the State to make progress toward a more security and stable enterprise

To the specific matter of legislation, I would like to frame our goal for the upcoming legislative session and hopefully solicit the committee's assistance in supporting a bill to centralize cybersecurity efforts. In

the 2017 legislative session, duplicate cybersecurity bills were introduced, Senate Bill 204 and House Bill 2331, now known as the Jim Morrison Cybersecurity Bill. Fortunately, both bills remain available. Of the two bills, House Bill 2331 was most active, however language was added that made the bill unacceptable to many. What I'm proposing is that we abandon House Bill 2331 and pursue Senate Bill 204 as the bill does not contain the additional language.

In response to Representative Curtis' question last session for details of how this solution would be delivered to all agencies small and large, services to the small agencies will be delivered in the same manner as services to the larger agencies, some already underway. Although the execution of the plan as a whole is dependent upon funding and legislation, neither of which we were successful in obtaining last legislative session, we have worked with the Executive Branch Chief Information Technology Officer to adjust in other areas to improve cybersecurity for all. In so doing, we have already begun to provide central cybersecurity resources to some Executive Branch state agencies. These additional services, included in their common network charge, include centralized logging, centralized vulnerability scanning and where practical firewall virtualization. In addition to these services, a late budget amendment of 2.6 million provided some funding that will allow us to address some additional cybersecurity shortcomings. Those items were presented in our last session.

It is important to note that though we have a published implementation approach, it was based on full funding and authorities from Legislation. This approach will need to be modified as partial monies from the appropriation and those realigned within the rates have allowed us to implement some provisions of the phased plan.

Thank you again for your time and consideration and I now stand for any questions you may have.