

Office of Information Technology Services  
900 SW Jackson  
Topeka, KS 66612 (785) 296-7440

Testimony of the Deputy Chief Information Security Officer  
IN SUPPORT OF HB 2509, STATE AGENCIES AND INFORMATION TECHNOLOGY PLANS  
Before the House Vision 2020 Committee  
February 10, 2016

I want to thank Chairman Campbell and members of the House Vision 2020 committee for the opportunity to speak to you today about House Bill 2509.

I am Rod Blunt, Deputy Chief Information Security Officer with the Office of Information Technology Services (OITS) and I'm here today to express my support for HB 2509.

I would like to begin my testimony by responding to the concerns expressed in neutral testimony offered on 3 February, 2016. Though not in opposition to the bill, concerns were expressed that decisions made under the authority granted by the bill may inadvertently cause security challenges for those organizations that either interface with criminal justice systems or cause security challenges for criminal justice organizations when interfacing with other government agencies.

In other neutral testimony it was offered that although security professionals from OITS were needed to completely re-engineer their security controls to pass a regulatory audit, no further assistance would be needed and that organization has since requested an exemption to this bill.

I applaud those coming forward and expressing their concerns, however I would like to take a moment to respond and hopefully remove or at least reduce those concerns. First, I would like to point out, and emphasize, the foundational tenants of information security, which are Integrity, Confidentiality and Availability. So, before any decision is made it must be fully vetted with all stakeholders to ensure compliance with these tenants, and all policy and regulatory requirements. Second, and probably more important, is the cause of this concern – which, in my opinion, is a lack of collaboration among organizations that share information today. What this bill promotes is interaction among security activities, something that is vital to developing a statewide efficient and effective information security program.

For agencies requesting an exemption, I would encourage them reconsider and I would also encourage this committee to reject these requests. There are numerous reports and studies supporting the benefits of a centralized security effort and many states, such as Virginia, Michigan, Oklahoma, Missouri, and Florida and many more across the nation have already completed the process and have metrics to prove the success of their efforts, none of which provided exemptions that I could find. I would challenge those agencies requesting exemptions to provide any studies, reports, or metrics substantiating their position and I would also inquire as to with whom they consulted to reach their conclusions and what their information security qualifications are.

Knowing the ever increasing threat, it's difficult to understand why any organization would want to exempt themselves from a resource that they can only benefit from. More important to the point is that by allowing these exemptions, we leave isolated pockets of agencies without any oversight, something

that is repeatedly found as a primary concern in Legislative Post Audit (LPA) reports and countless data breach reports.

Furthermore, my sense is that there is an underlying concern that centralizing security would either cannibalize personnel and organizational resources, or increase current service rates, which is simply not the case. To alleviate these concerns I would encourage another review of the amended bill, as well as the revised fiscal note and the Information Security Strategic Plan or contact me directly for clarity. I hope that this response dispels those concerns and turns neutral testimony into proponent testimony.

One of the questions posed by the committee on February 3, was whether or not new statute language is necessary to correct deficiencies in information security or could an Executive Order accomplish the same. To answer this question I would ask the committee to consider the volume, and repeated findings in LPA reports on information security spanning many years. The repetitious findings suggest a more systemic problem and something more substantive and permanent is necessary to overcome a growing level of risk across State government.

I would like to add that I've served the citizens of Kansas for more than thirteen years, ten of which has been dedicated to information security and I cannot emphasize enough how important this legislation is to the families and businesses of Kansas. Unless you've been a victim of computer crime such as identity theft, one cannot understand the hardship suffered for many years after; it's extremely difficult to overcome. With the passage of this legislation we can begin to develop a security program to overcome years of repeated vulnerabilities and reduce our collective risk to cyber crime.

In conclusion, I would echo the testimony of the Executive CITO, Phil Wittmer, that "the benefits of centralizing information security present a clear benefit for the State of Kansas". I would like to thank the committee for their time and opportunity to present this testimony and I urge the committee to support HB 2509.