B&CB

SC BUDGET AND CONTROL BOARD

Senate Finance Committee

Comments on S. 334

Jimmy Earley
Division of State Information Technology

February 12, 2013

Comments on S. 334

- **Structure**
- SC, to my knowledge, would be the only state with a cabinet level agency dedicated to information security and a CISO that reports directly to the Governor.
- Most state CISOs work within the state IT organization and report to the state CIO.
- In other organizations the CISO may report to someone outside of IT, but the CISO and CIO report to the same person.
- In order to balance operational and security considerations, it may be advisable to have the state CIO and the state CISO report to the same person (e.g. Governor, DOA Director, Budget and Control Board Director).

Comments on S. 334

- Recommend that the following authority be given to the Chief Information Security Officer. This authority will allow the CISO to be as proactive as possible in managing the safety of state systems:
- Procurement – Involve the CISO in IT procurements - The State CISO should have authority to review and approve agency IT procurement requests.

Comments on S. 334

- Compliance – Give the CISO the authority to audit agencies for compliance with standards and policies/procedures. This would include audits of new systems/new projects PRIOR to implementation. It will be helpful to have CISO involved early in major IT projects.

Comments on S. 334

- Allow the CISO to perform IV&V functions on new software development projects (review and oversee software development from a security perspective).
- Require the CISO to create an Enterprise Security Architecture. The architecture may be defined as the security design and identifies the specific controls (technology) that will be put in place. Polices, practices and standards all stem from the overall architecture. May be helpful to also give the CISO authority to sunset certain practices/technology that are not consistent with new standards/polices.

Comments on S. 334

- The CISO should have specific authority to create standards and practices that govern use of third party contractors that work for agencies and have access to sensitive data.
- CISO should be empowered to conduct risk assessments as necessary in order to identify/measure risks
- CISO should be required to develop an annual Security plan (action plan and budget, resource requirements to address known risks)

Comments on S. 334

- CISO should be responsible for directing forensic work (collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law).
- CISO should be responsible for managing incident responses

Comments on S. 334

- There are non-system related threats that must also be managed. For example, internal threats, physical security requirements and disaster recovery risks. The CISO should be authorized to develop strategies and create polices and practices to address these types of risks as well.
- The CISO should be authorized to offer security services to state agencies (such as conducting threat assessments, penetration testing, network monitoring, etc.)

Comments on S. 334

Article 3 – Technology Investment Council

- It may be beneficial for a representative from the State Budget Office to serve on the Council