Cybersecurity Workshop
Joint Session with NASS,
Anchorage, Alaska
July 20, 2013

Douglas Robinson, Nat'l Assoc of State Chief Information Officers
Jayne Friedland Holland, NIC

Cyber security – states have become attractive targets of criminally based organizations for both data theft and identity theft. Data breeches are more common.

Growing security risks are the use of personally-owned devices used for state business, cloud resources, malicious software, "spear fishing" attacks: use of e-mail w/ embedded links that, if clicked, load malicious software, malware.

Important to make sure that antivirus software is up-to-date.

Budgets: security is not protected from cuts. Lack of funding diminishes cyber security efforts. States should spend 5% of their IT budgets on security, but in reality the figure is more like 1-2%.

There are not enough cyber security professionals possessing necessary certification.

Cloud concerns. Third-party providers. States using cloud services have less control over their data, where and how it is stored. Questions: Do states have cyber security frameworks with security metrics and testing? Continuous vulnerability management? What does security look like?

Service level agreements with Cloud providers are usually one-sided favoring the Cloud Providers. States need to have their Cloud service level agreements reviews by their Attorney Generals offices. Agreements need to include such things as data security, access, data ownership, records retention. What happens in the event of data breech, loss or damage? interruption of service, sub-contracting, system down time? Specification as to what security looks like.