Dennis Cobb_2/21/14

Notional Information Security Taxonomy

Sharing sensitive business and personal information is vital to countless transactions in modern life. Public confidence in sharing such information is a critical element business and government operations that rely on this data to perform their purpose. This conceptual framework is proposed as a means to achieve common understanding in NV about how sensitive information should be protected. It is not meant to supercede other information designations, but rather to provide a means for people to know their obligations in storing, transmitting, or disposing of such information.

Efficient operations can benefit from common standards and a shared understanding of the sensitivity of information to unauthorized dissemination, as well as shared acknowledgement of responsibilities in securing that data. A conceptual framework mapping information sensitivity to corresponding security requirements can facilitate confident, efficient information handling for Nevada businesses and governments.

- **Tier I:** Tier I information is sufficient by itself to allow inflict loss, disruption or harm. Disclosure of Tier I information to unauthorized parties will cause loss, disruption or harm to people or organizations including, but not limited to, financial loss, identity theft, or loss of intellectual property.

  Tier I information will be encrypted to a minimum of [...] when stored or transmitted, and will be disposed of through overwriting with zeros [X] times or physical destruction of the storage medium.

- **Tier II:** Tier II information can be combined with other public or private information to inflict loss, disruption or harm. Disclosure of Tier II information to unauthorized parties may cause disruption or harm to people or organizations including, but not limited to, financial loss, identity theft, or loss of intellectual property.

  Tier II information will be encrypted to a minimum of [...] when stored or transmitted, and will be disposed of through overwriting with zeros [X] times or physical destruction of the storage medium.

- **Tier III:** Tier III information is proprietary or personal information that cannot readily be combined with other public or private information to inflict loss, disruption or harm. Disclosure of Tier III information to unauthorized parties may disclose private information, but is unlikely to cause loss, disruption or harm to people or organizations.

  Tier III information may be encrypted to a minimum of [...] when stored or transmitted, and should be disposed of through overwriting with zeros [X] times or physical destruction of the storage medium.