Introduction to Dropbox

Jim Miller, LCITO

Office 785.296.5566

Mobile 913.484.8013

Email jim.miller@las.ks.gov

Introduction to Dropbox

- What is it?
- Why use it?
- Mitigating the risks of using Dropbox?
- Dropbox – How does it work?
- Quick demo of Dropbox
- Questions?

Attachment: Background info on Amazon Web Services

Dropbox – What is it?

- **Tool that helps you manage and share files**
  - PDFs, MSWord docs, MSExcel docs, photos, etc.
- **Access files from multiple devices**
  - From all of your electronic devices: state laptop, Apple laptop, home computer, tablet, smartphone
- **Share files and access to files with others**
  - Push files to other Dropbox users
    or
  - Provide links to enable online access

Dropbox – Why use it?

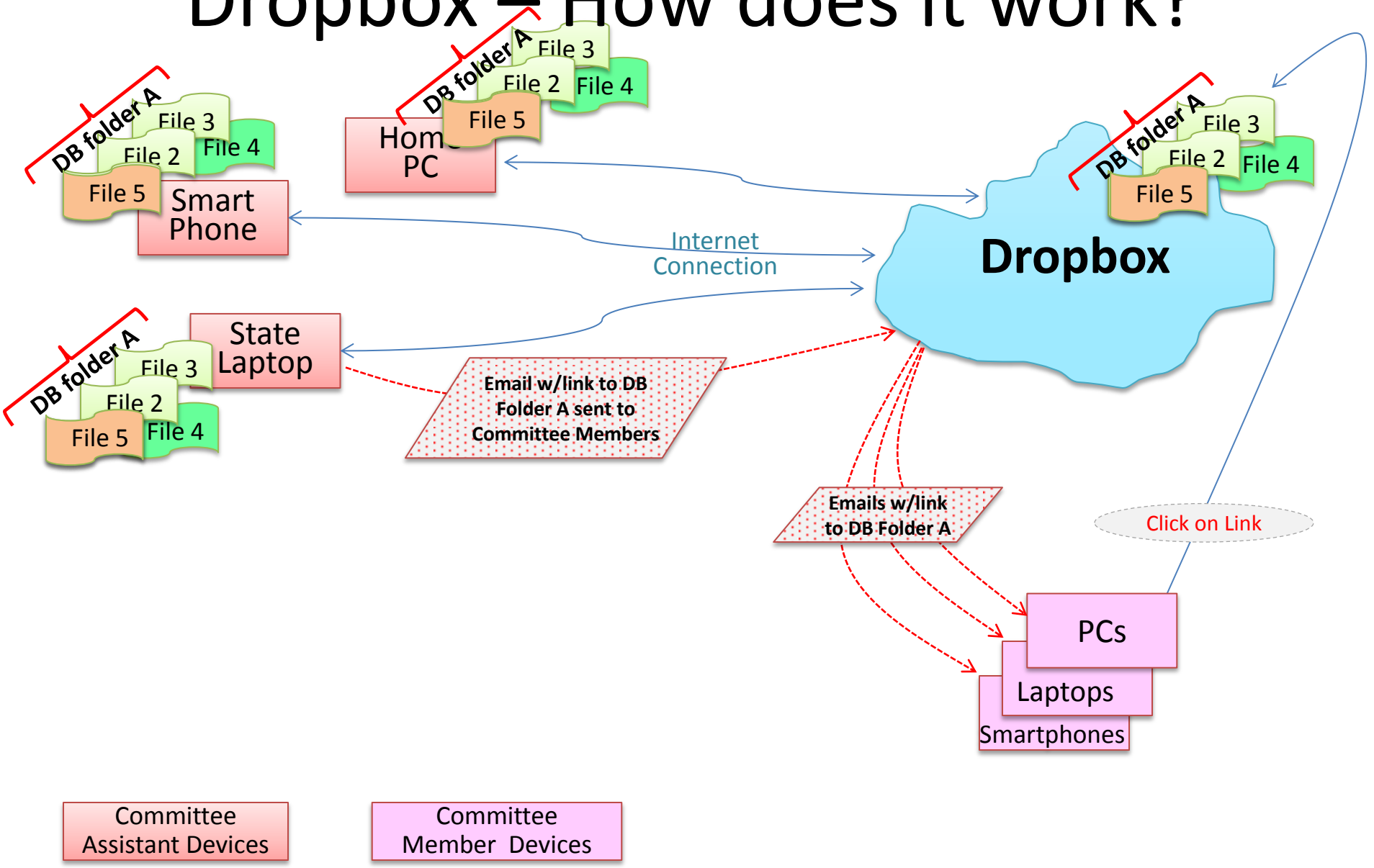
- **Individual:** Enable access to your own files
  - From all of your electronic devices
  - Sync files across all your devices

- **Committee:** Share files with others
  - Manage file sharing with Committee members
  - Enable file sharing beyond the Legislature
  - Efficient, controlled sharing from one point
  - Effective, open access with one tool

Mitigating the risks of using Dropbox?

- **KORA and KOMA**
- **Use Dropbox for:**
  - Sharing files normally shared with the Committee
  - Accessing shared files from your different devices
- **Do not use Dropbox for:**
  - Communicating with fellow Committee members
  - Collaborating with fellow Committee members re individual edits, views, decisions, etc.

Dropbox – How does it work?



Dropbox

Quick demo

Dropbox

Questions?

Background info re Amazon Web Services (AWS), providers of the Dropbox service.

Amazon Web Services (AWS) delivers a highly scalable cloud computing platform with high availability and dependability, and the flexibility to enable customers to build a wide range of applications. The issues of end-to-end security and end-to-end privacy within the cloud computing world are more sophisticated than within a single data center not facing the Internet. Ensuring the confidentiality, integrity, and availability of customer's systems and data is of the utmost importance to AWS, as is maintaining trust and confidence. **Security Overview**

We provide this overview so that you can better understand the security measures we've put in place to protect the information that you store using Dropbox.

Secure Storage

We encrypt the files that you store on Dropbox using the AES-256 standard, which is the same encryption standard used by banks to secure customer data. Encryption for storage is applied after files are uploaded, and we manage the encryption keys.

Dropbox uses Amazon S3 for data storage. Amazon stores data over several large-scale data centers. According to Amazon, they use military grade perimeter control berms, video surveillance, and professional security staff to keep their data centers physically secure.

You can find more information about Amazon's security at the Amazon Web Services' website.

Amazon and Dropbox also employ significant protection against network security issues such as Distributed Denial of Service (DDoS) attacks, Man in the Middle (MITM) attacks, and packet sniffing.

Secure Transfers

Your files are sent between Dropbox's desktop clients and our servers over a secure channel using 256-bit SSL (Secure Sockets Layer) encryption, the standard for secure Internet network connections.

Your files are sent between Dropbox's mobile apps and our servers over a secure channel using 256-bit SSL encryption where supported. Not all mobile media players support encrypted streaming, so media files streamed from our servers are not always encrypted.

Your Data is Backed Up

Dropbox and Amazon keep redundant backups of all data over multiple locations to prevent the remote possibility of data loss. In the unlikely event that this redundancy were to fail, Dropbox folders linked to a desktop computer client will still contain copies of your files (except files you've chosen not to sync using Selective Sync).

Privacy

A copy of our full privacy policy can be found at: https://www.dropbox.com/privacy.

We guard your privacy to the best of our ability and work hard to protect your information from unauthorized access.

Dropbox employees are prohibited from viewing the content of files you store in your Dropbox account, and are only permitted to view file metadata (e.g., file names and locations). Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so). But that's the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances. In addition, we employ a number of physical and electronic security measures to protect user information from unauthorized access.