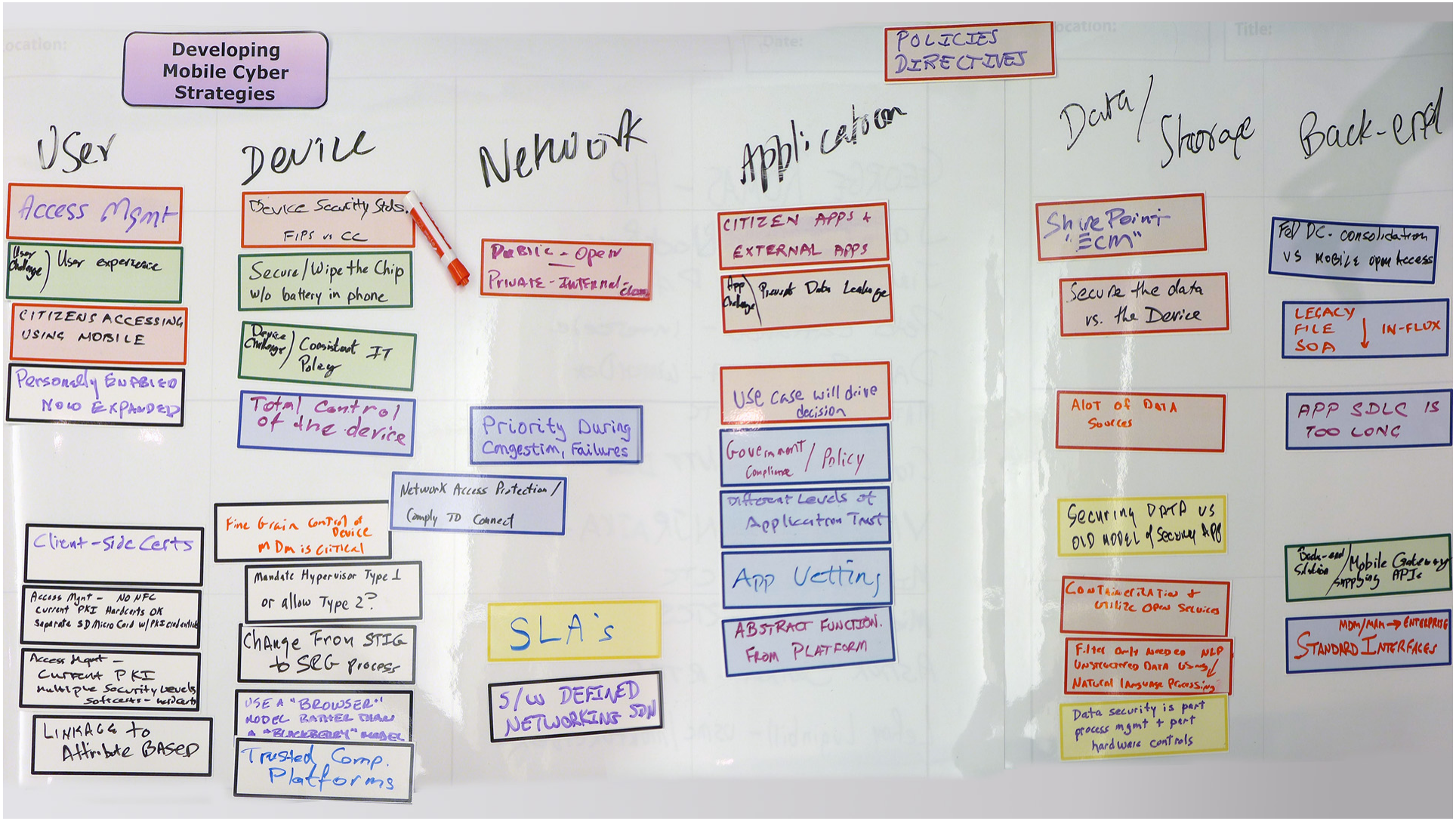
2013 Federal Mobile Collaborative Sessions

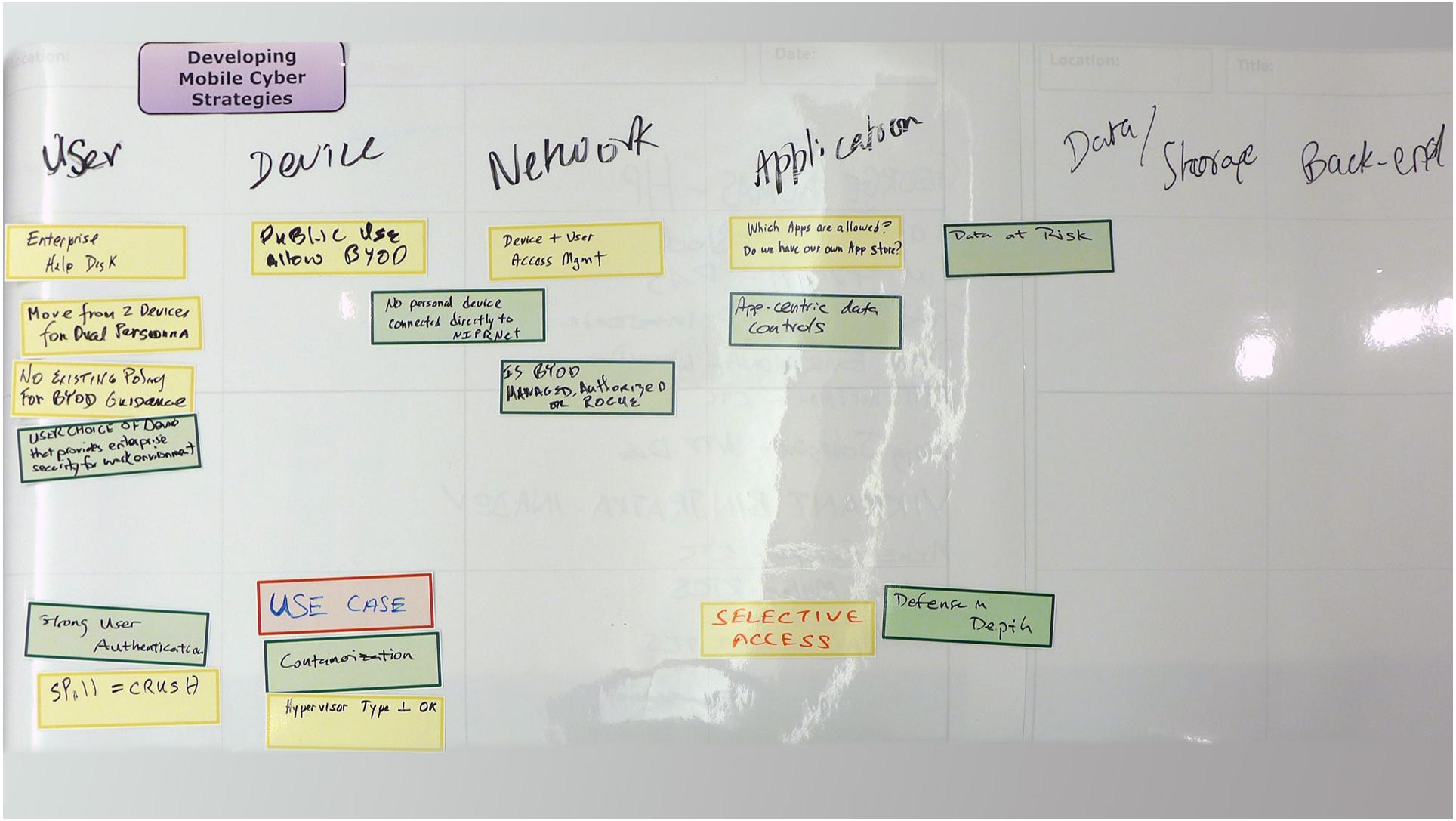
July 8th

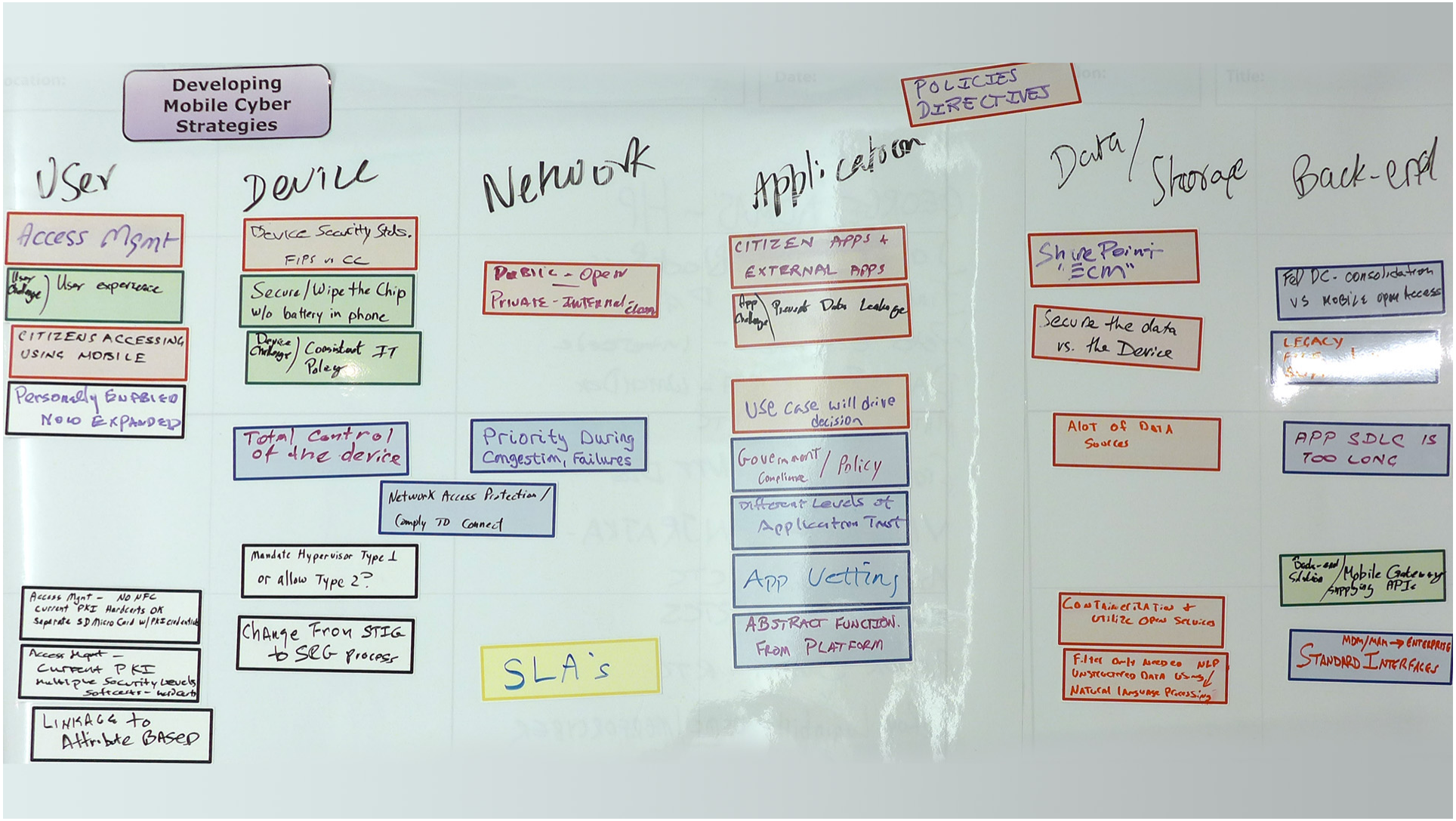
Developing Mobile Cyber Strategies

Collaborative Lead:

Ashok Sankar


Developing Mobile Cyber Strategies
POLICIES DIRECTIVES
User
Device
Network
Application
Data / Storage
Back-end
Access Mgmt
User Challenge / User experience
CITIZENS ACCESSING USING MOBILE
Personally ENABLED NOW EXPANDED
Client-Side Certs
Access Mgmt - NO NFC current PKI Hardcerts OK Separate SD Micro Card w/ PKI credentials
Access Mgmt - Current PKI multiple Security Levels Softcerts - Hardcerts
LINKAGE to Attribute BASED
Device Security Stds. FIPS vs CC
Secure / Wipe the Chip w/o battery in phone
Device Challenge / Constant IT Policy
Total Control of the device
Fine Grain Control of Device MDM is Critical
Mandate Hypervisor Type 1 or allow Type 2?
Change From STIG to SRG Process
USE A "BROWSER" MODEL RATHER THAN A "BLACKBERRY" MODEL
Trusted Comp. Platforms
PUBLIC - Open
PRIVATE - INTERNAL Cloud
Priority During Congestion, Failures
Network Access Protection / Comply TO Connect
SLA's
S/W DEFINED NETWORKING SDN
CITIZEN APPS + EXTERNAL APPS
App Challenge / Private Data Leakage
Use case will drive decision
Government Compliance / Policy
Different Levels of Application Trust
App Vetting
ABSTRACT FUNCTION. FROM PLATFORM
SharePoint "ECM"
Secure the data vs. the Device
A lot of Data Sources
Securing DATA vs OLD MODEL of Securing APP
CONTAINERIZATION + Utilize Open Services
Filter Only Needed NLP Unstructured Data Using Natural Language Processing
Data security is part process mgmt + part hardware controls
Fed DC - consolidation vs Mobile open access
LEGACY FILE SOA ↓ IN-FLUX
APP SDLC IS TOO LONG
Back-end Services / Mobile Gateway Supporting APIs
MDM/MAM → ENTERPRISE STANDARD INTERFACES


Developing Mobile Cyber Strategies
User
Device
Network
Application
Data/Storage
Back-end
Enterprise Help Desk
Move from 2 Devices for Dual Persona
NO EXISTING POLICY FOR BYOD GUIDANCE
USER CHOICE OF DEVICE that provides enterprise security for work environment
Public Use Allow BYOD
No personal device connected directly to NIPRNet
Device + User Access Mgmt
ES BYOD MANAGED, Authorized OR ROGUE
Which Apps are allowed? Do we have our own App store?
App-centric data controls
Data at Risk
Strong User Authentication
SPoF = CRUSH
USE CASE
Containerization
Hypervisor Type 1 OK
SELECTIVE ACCESS
Defense in Depth


Developing Mobile Cyber Strategies
POLICIES DIRECTIVES
User
Device
Network
Application
Data / Storage
Back-end
Access Mgmt
User Challenge
User experience
CITIZENS ACCESSING USING MOBILE
Personally Enabled Now Expanded
Device Security Stds. FIPS vs CC
Secure/Wipe the Chip w/o battery in phone
Device Challenge
Consistent IT Policy
Total Control of the device
Mandate Hypervisor Type 1 or allow Type 2?
CHANGE From STIG to SRG process
PUBLIC - Open
PRIVATE - INTERNAL - class.
Priority During Congestion, Failures
Network Access Protection / Comply TO Connect
SLA's
CITIZEN APPS + EXTERNAL APPS
App Challenge
Prevent Data Leakage
USE case will drive decision
Government / Policy Compliance
Different Levels of Application Trust
App Vetting
ABSTRACT FUNCTION. FROM PLATFORM
SharePoint "ECM"
Secure the data vs. the Device
ALOT of DATA Sources
CONTAINERIZATION + Utilize OPEN Services
Filter Only NEEDED NLP UNSTRUCTURED DATA USING / NATURAL LANGUAGE PROCESSING
Fed DC - consolidation VS MOBILE OPEN ACCESS
LEGACY
APP SDLC IS TOO LONG
Back-end Solution / Mobile Gateway Supporting APIs
MDM/MAM → ENTERPRISE STANDARD INTERFACES
Access Mgmt - NO NFC current PKI Hardcerts OR Separate SD Micro Card w/ PKI credentials
Access Mgmt - CURRENT PKI multiple Security Levels Softcerts - Hardcerts
LINKAGE to Attribute BASED