Mobile Device Security Checklist

NNSA IMC Conference

April 19, 2012

Lee Neely, CISSP CCUV

Lawrence Livermore National Laboratory

LLNL-PRES-543811

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

Agenda

- Background and Goals of the Checklist
- Areas to Consider
- Expansion of some topics
  - Device Management
  - Device Verification
  - Device Lifecycle
  - Policies
  - Risk Management
- Base Security Settings
- App provisioning
- BYOD
- App Development and Hacking

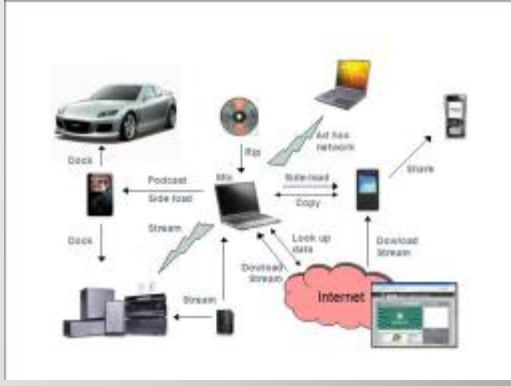
Background & Goals

- Mobility is now pervasive
  - Critical to attracting new talent
  - Critical to modern mission delivery
  - Opting out is not viable
- A common approach to securing devices is needed
  - Devices and device options vary
    - New devices are always “en route”
  - Goals remain the same
    - Provide functionality
    - Protect corporate information
    - Provide assurance device and users are following the rules

Background & Goals

- Checklist is designed to take you from “Zero to Hero”
- Checklist spans many areas impacted by mobility
- Designed to be repeatable regardless of technology
  - “Device Agnostic”
- Doesn’t solely rely on technology to mitigate risk

Areas to Consider



- Start with use cases
  - Have to understand how the devices are to be used
  - Be sure to capture edge cases
- Identify the Risks and Mitigations
  - Perform a risk assessment
    - Identify technical and administrative controls
  - Pay particular attention to information protection and migration
  - Review and update existing mitigations
- Review policies
  - Add/update where needed to support controls

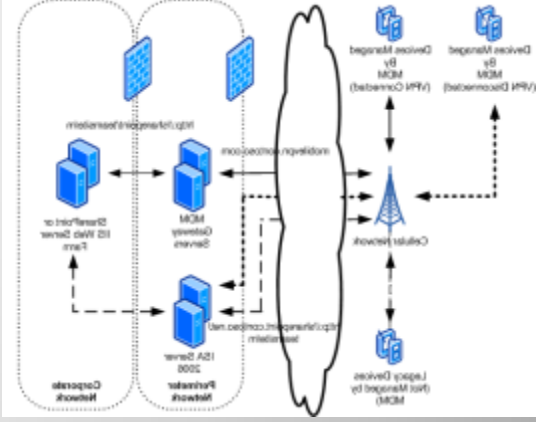
Areas to Consider

- Review training
  - Add/Update where needed, find and fill gaps
  - Users need to know expectations and requirements
  - Ensure training aligned with policies and mitigations
- Device Management
- Device Verification
- Device Lifecycle

Areas to Consider

- AV solution
  - Some devices support and need AV e.g. Android
- Application deployment model
  - Controlled or free-for-all
- Synchronization
  - What is permitted
  - Understand the security implications of
    - Cloud synchronization
    - Desktop synchronization
    - Ad-Hoc synchronization

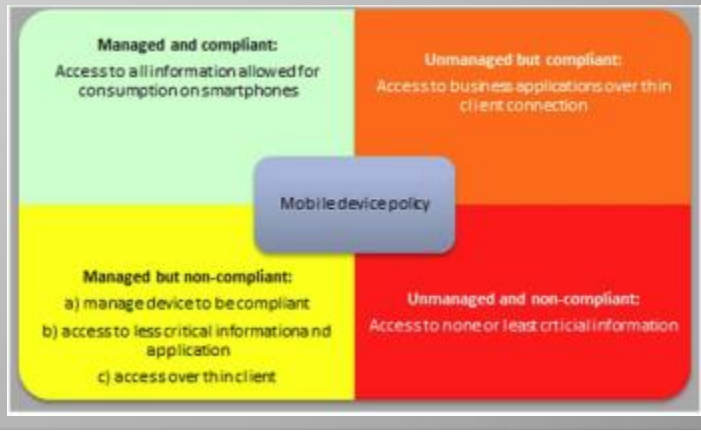
Device Management



- Select device operation model
  - Sandbox, whole device or hybrid
- Select and implement MDM solution
- Select security settings to match technical controls
  - Review existing guides (NSA, DISA, …) – often easier than starting from scratch
  - Tailor to meet needs
- Validate implementation of controls

Device Verification

- Audit Configuration
  - Is device operating within bounds
  - Are security settings still in effect
  - Are applications within corporate limits
  - Trust but Verify

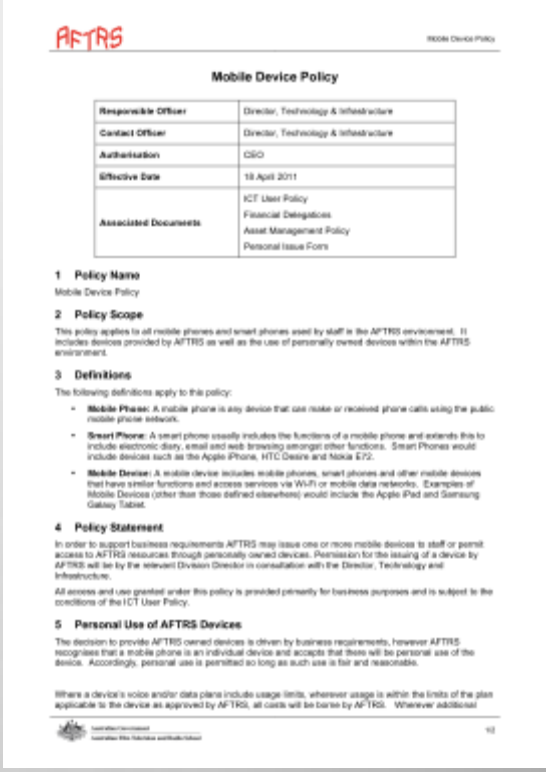


Device Lifecycle

- Devices have a life of 18 months or less
- Corresponding procedures/processes
  - Device provisioning procedure
    - Procurement/Enrollment/Provisioning
  - Device reuse procedure
  - Device software update procedure
  - Device disposal procedure
  - New (model/version) device procedure
    - Acceptance/validation

Policies to consider

- Use of the camera
- Use of voice recording
- Application purchases
  - Market/store purchases
  - In-App purchases
  - Free apps
- Incidental use
- Encryption at rest
- Autoconnect to Wi-Fi
- Use restrictions
- File sharing/use of cloud services



AFTRS

Mobile Device Policy

Responsible Officer	Director, Technology & Infrastructure
Contact Officer	Director, Technology & Infrastructure
Authorisation	CEO
Effective Date	18 April 2011
Associated Documents	ICT User Policy Financial Delegations Asset Management Policy Personal Issue Form

1 Policy Name

Mobile Device Policy

2 Policy Scope

This policy applies to all mobile phones and smart phones used by staff in the AFTRS environment. It includes devices provided by AFTRS as well as the use of personally owned devices within the AFTRS environment.

3 Definitions

The following definitions apply to this policy:

- **Mobile Phone:** A mobile phone is any device that can make or received phone calls using the public mobile phone network.
- **Smart Phone:** A smart phone usually includes the functions of a mobile phone and extends this to include electronic diary, email and web browsing amongst other functions. Smart Phones would include devices such as the Apple iPhone, HTC Desire and Nokia E72.
- **Mobile Device:** A mobile device includes mobile phones, smart phones and other mobile devices that have similar functions and access services via Wi-Fi or mobile data networks. Examples of Mobile Devices (other than those defined elsewhere) would include the Apple iPad and Samsung Galaxy Tablet.

4 Policy Statement

In order to support business requirements AFTRS may issue one or more mobile devices to staff or permit access to AFTRS resources through personally owned devices. Permission for the issuing of a device by AFTRS will be by the relevant Division Director in consultation with the Director, Technology and Infrastructure.

All access and use granted under this policy is provided primarily for business purposes and is subject to the conditions of the ICT User Policy.

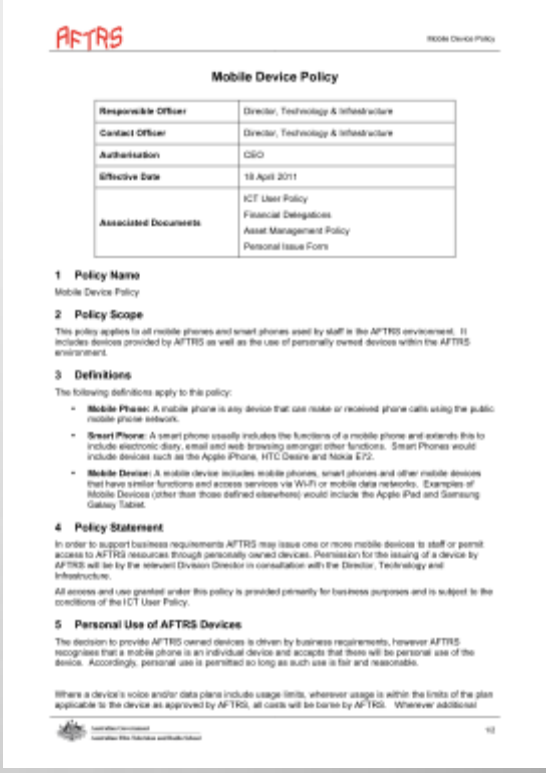
5 Personal Use of AFTRS Devices

The decision to provide AFTRS owned devices is driven by business requirements, however AFTRS recognises that a mobile phone is an individual device and accepts that there will be personal use of the device. Accordingly, personal use is permitted so long as such use is fair and reasonable.

Where a device's voice and/or data plans include usage limits, wherever usage is within the limits of the plan applicable to the device as approved by AFTRS, all costs will be borne by AFTRS. Wherever additional

Policies to consider

- Bluetooth
  - Pairing
  - Discoverable
  - Limits on devices paired with
- VPN use and impact
- Password
- Lost or Stolen device reporting and actions
- Physical security when not in use
- Connection of device to non-corporate devices
- Location services
- Storage and transmission of sensitive information
  - Alternate data paths: Email, Cloud, etc.



AFTRS

Mobile Device Policy

Responsible Officer	Director, Technology & Infrastructure
Contact Officer	Director, Technology & Infrastructure
Authorisation	CEO
Effective Date	18 April 2011
Associated Documents	ICT User Policy Financial Delegations Asset Management Policy Personal Issue Form

1 Policy Name

Mobile Device Policy

2 Policy Scope

This policy applies to all mobile phones and smart phones used by staff in the AFTRS environment. It includes devices provided by AFTRS as well as the use of personally owned devices within the AFTRS environment.

3 Definitions

The following definitions apply to this policy:

- **Mobile Phone:** A mobile phone is any device that can make or received phone calls using the public mobile phone network.
- **Smart Phone:** A smart phone usually includes the functions of a mobile phone and extends this to include electronic diary, email and web browsing amongst other functions. Smart Phones would include devices such as the Apple iPhone, HTC Desire and Nokia E72.
- **Mobile Device:** A mobile device includes mobile phones, smart phones and other mobile devices that have similar functions and access services via Wi-Fi or mobile data networks. Examples of Mobile Devices (other than those defined elsewhere) would include the Apple iPad and Samsung Galaxy Tablet.

4 Policy Statement

In order to support business requirements AFTRS may issue one or more mobile devices to staff or permit access to AFTRS resources through personally owned devices. Permission for the issuing of a device by AFTRS will be by the relevant Division Director in consultation with the Director, Technology and Infrastructure.

All access and use granted under this policy is provided primarily for business purposes and is subject to the conditions of the ICT User Policy.

5 Personal Use of AFTRS Devices

The decision to provide AFTRS owned devices is driven by business requirements, however AFTRS recognises that a mobile phone is an individual device and accepts that there will be personal use of the device. Accordingly, personal use is permitted so long as such use is fair and reasonable.

Where a device's voice and/or data plans include usage limits, wherever usage is within the limits of the plan applicable to the device as approved by AFTRS, all costs will be borne by AFTRS. Wherever additional

Risk Management

- Device Access (lost devices)
  - Off-network
  - On-network
  - Casual access attempt
  - Forensic access
  - Jailbreak/Hack
- Malicious Code
  - Apps with extra access/features
  - Apps with overt access/features
  - Apps with incomplete security
- Security Settings
  - Bugs in vendor implementation
  - User removes settings
- Device and Data access
  - Single User or All users model
  - Bluetooth
  - MITM – SSL, Wi-Fi, etc.
  - Incomplete encryption
- Hot Mic
- Data Loss Prevention
  - Copy and Paste
  - Attachment sharing
  - Email data migration
  - Cloud Storage

Beginning Security Settings

- Device diversity drives general suggestions
- Prevent easy removal of corporate security settings
- Password
  - strength, reuse restrictions, change interval
- Device auto-lock
- Encrypt device backup
- Enable remote wipe/locate/lock
- Enable device encryption
- Corporate VPN and Wi-Fi configuration
- Disable cloud storage and backup

Application provisioning

- Centrally provisioned Apps
- Application approval
  - Understand
    - business need
    - functions and connections, overt and hidden
  - Evaluate source (Author)
  - White or Black list
- Application Purchase account & process
  - Corporate or Personal persona
  - Re-imbursement process
- Application Source
  - Pushed? Market/App store? Corporate App Store?

So you want BYOD?

- BYOD – repeat the checklist
  - Make sure you understand what BYOD means to you
  - What level of processing is acceptable in BYOD?
  - How does that impact information protection?
  - Update use cases
  - Update risk assessment
  - Update policies, training
  - Review MDM solution, Security settings, …
  - Consider sandbox to protect information
  - Device Lifecycle

Application Development

- Mobile device application development is a new discipline
  - Guidance is evolving
    - Perform Risk Assessment
    - Develop secure coding, testing and acceptance process
- Secure the App, make it self-defending
  - Use integrity checks of the application and the device
  - Protect (encrypt) any data or credentials stored on the device
- Consider the distribution channel
  - Do you want just anyone downloading and interrogating your App?

Mobile App Hacking 101

- Devices hacked or jailbroken
- Framework installed to hide device compromise from apps with compromise detection
- Apps then run with debugger attached
- App internals, security code (and exploit) then published to hacker social networks
- Developer patches App
- Repeat…

References

- **Mobile device checklist:**
  - http://www.sans.org/score/mobile-device-checklist.php
- **iOS Platform Security Guide:**
  - http://www.sans.org/score/ios-platform-sec_checklist.php
- **SANS RSA Reference:**
  - http://www.scmagazine.com.au/News/292784,the-six-most-dangerous-infosec-attacks.aspx
- **SANS SEC 571 Mobile Device Security:**
  - https://www.sans.org/security-training/mobile-device-security-5021-tid
- **MDM Solutions comparison**
  - **Full Device**
    - http://www.enterpriseios.com/wiki/Comparison_MDM_Providers
  - **Sandbox**
    - http://www.enterpriseios.com/wiki/Sandbox_Environments
- **Mobile Device Baseline Configurations:**
  - **DISA STIGS:**
    - http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html
  - **CIS Benchmarks**
    - https://benchmarks.cisecurity.org/en-us/?route=community.projects
- **Mobile Device Security Software Comparison**
  - http://mobile-security-software-review.toptenreviews.com/

References

- **Australian Defense Signals Directorate iOS Hardening guide**
  - http://www.dsd.gov.au/publications/iOS5_Hardening_Guide.pdf

- **Android vs. iOS: security Comparison**
  - http://palpapers.plynt.com/issues/2011Oct/android-vs-ios/

- **“Infographic” Android/iOS comparison from Redmond Pie**
  - http://www.redmondpie.com/android-vs.-ios-how-secure-are-they-infographic/

Questions?

My contact information:
Lee Neely, CISSP CCUV
Email: neely1@llnl.gov
Phone: (925) 422-0140