NIST Mobile Security Guidance Updates

Gema Howell, NIST

ATARC Federal Mobile Technology Summit

August 30, 2018

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

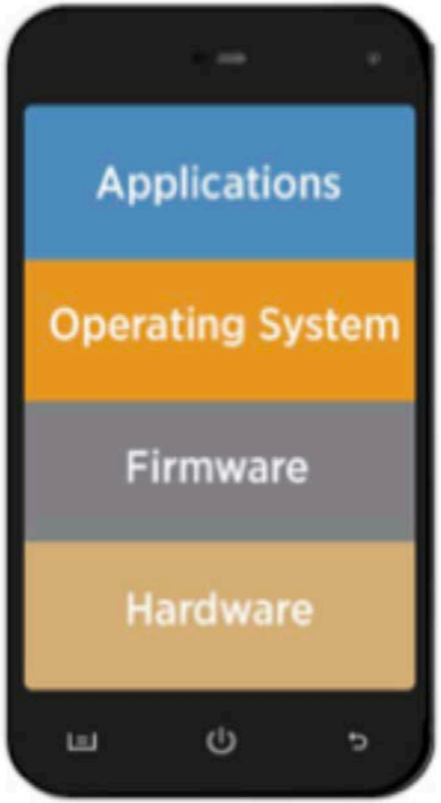
NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Agenda

- Applicable NIST Guidance
- NIST SP 800-124 Updates
- NCCoE Mobile Device Security Building Block

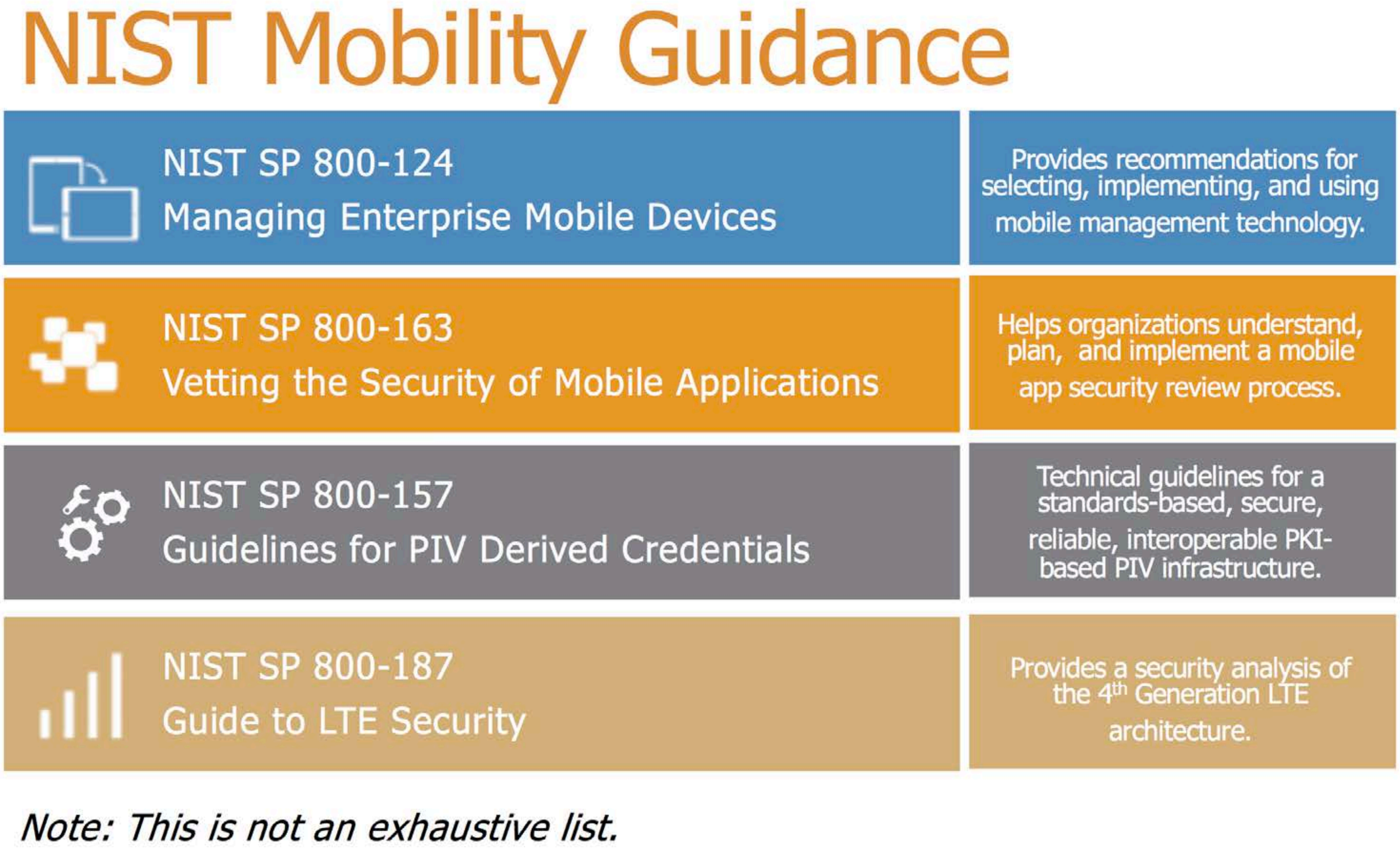
Mobile Device Definition

- No unified federal definition
- *NIST 800-53 Rev 4 Definition*
  - A portable computing device that has:
    - small form factor
    - wireless communication capabilities
    - local data storage
    - self- contained power source.



[NIST 800-53 Rev. 4 Definition]

OVERVIEW OF CURRENT EFFORTS



NIST Mobility Guidance

NIST SP 800-124 Managing Enterprise Mobile Devices	Provides recommendations for selecting, implementing, and using mobile management technology.
NIST SP 800-163 Vetting the Security of Mobile Applications	Helps organizations understand, plan, and implement a mobile app security review process.
NIST SP 800-157 Guidelines for PIV Derived Credentials	Technical guidelines for a standards-based, secure, reliable, interoperable PKI-based PIV infrastructure.
NIST SP 800-187 Guide to LTE Security	Provides a security analysis of the 4th Generation LTE architecture.

Note: This is not an exhaustive list.

800-124 Table of Contents

Old (2013)

- Purpose and Scope
- Mobile Device Characteristics
- Threats and Vulnerabilities
- Management Technologies Characteristics
- Mobile Device Lifecycle

New (2018)

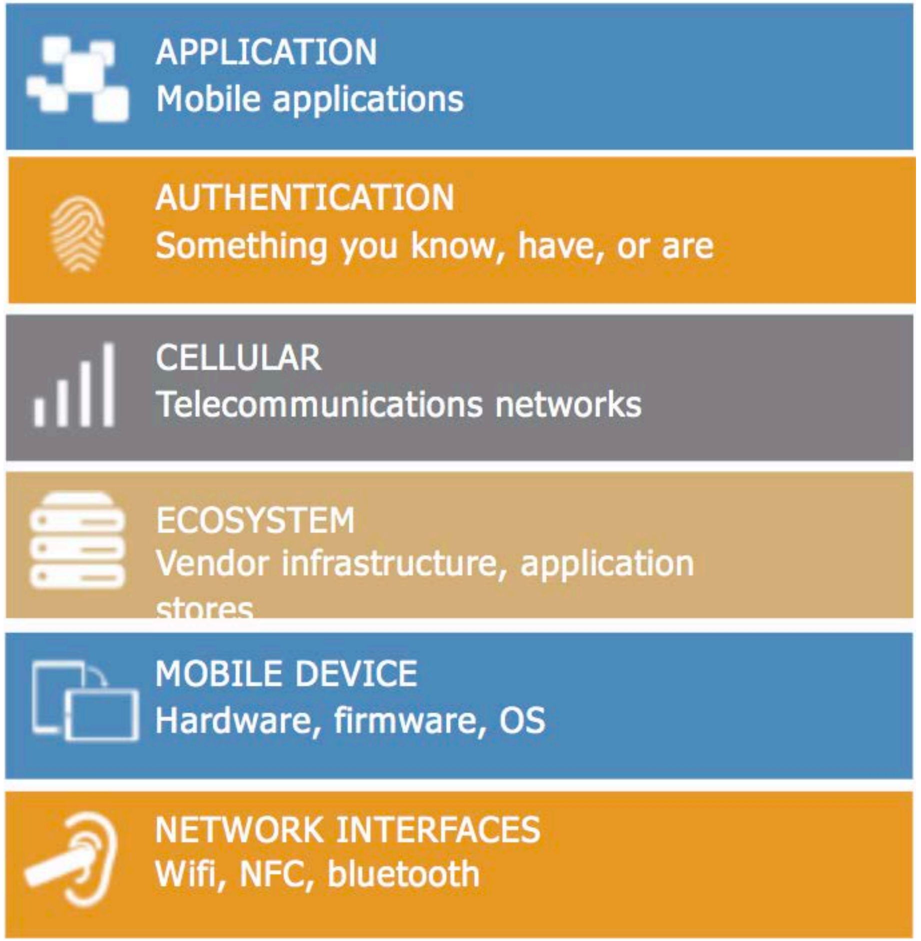
- Purpose and Scope
- Mobile Device Characteristics
- **Management Technologies Characteristics**
- **Deployment Considerations**
- **Threats to Mobile System**
- **Mitigations**

New Management Technologies Characteristics

- New EMM / MDM Capabilities
- Application Vetting
- Malware Detection
- Mobile Threat Intelligence
- Network and Host Vulnerability Scanning
- VPNs (e.g., per-app, OS, captive portals)
- Unified Endpoint Management (UEM)
- App Stores and Enterprise Apps

Expansion of the Threat Model

- Describe High-level Threats
- Interoperate with the NIST Mobile Threat Catalogue
- Privacy Implications
- Threat Categories



APPLICATION
Mobile applications

AUTHENTICATION
Something you know, have, or are

CELLULAR
Telecommunications networks

ECOSYSTEM
Vendor infrastructure, application stores

MOBILE DEVICE
Hardware, firmware, OS

NETWORK INTERFACES
Wifi, NFC, bluetooth

Old Appendices

- NIST SP 800-53 control sets and related publications
- Mobile device security-related checklists

New Appendices

- NIST SP 800-53 control sets
  - **Mapped to the various enterprise mobile security technologies**
- **New recommended MDM configurations**
- **OS-agnostic device configurations**

MOBILE DEVICE SECURITY FOR ENTERPRISES @NCCOE

1800-4: Cloud & Hybrid Build (2014)

Demonstrate commercially available mobility management technologies:

- **Securely enable basic email, calendar and contacts**
- Allowing for granular control over the enterprise network boundary
- Minimizing the impact on function

Mobile Threat Catalogue

- Identify threats to devices, applications, networks, & infrastructure
- Collect countermeasures that IT security engineers can deploy to mitigate threats
- Inform risk assessments
- Build threat models
- Enumerate attack surface for enterprise mobile systems
- Assist in standards mapping activities

NISTIR 8144: Assessing Threats to Mobile Devices & Infrastructure

MDSE Builds

- ***Build 1*** – Fully-managed device - strong data confidentiality is implemented using federally certified and validated technologies
- ***Build 2*** – BYOD - business productivity tools are deployed alongside a variety of device policies for employees with different risk profiles

Build 1

- Due in the beginning of next year
- Focused on federal standards and policies
- Use of NIST Risk Management Framework applied to a mobility use case
- Primarily focused on a reference for 800-124
  - Also incorporated other NIST pubs like 800-163
  - NIST Privacy Risk Assessment Framework

Partners

MobileIron

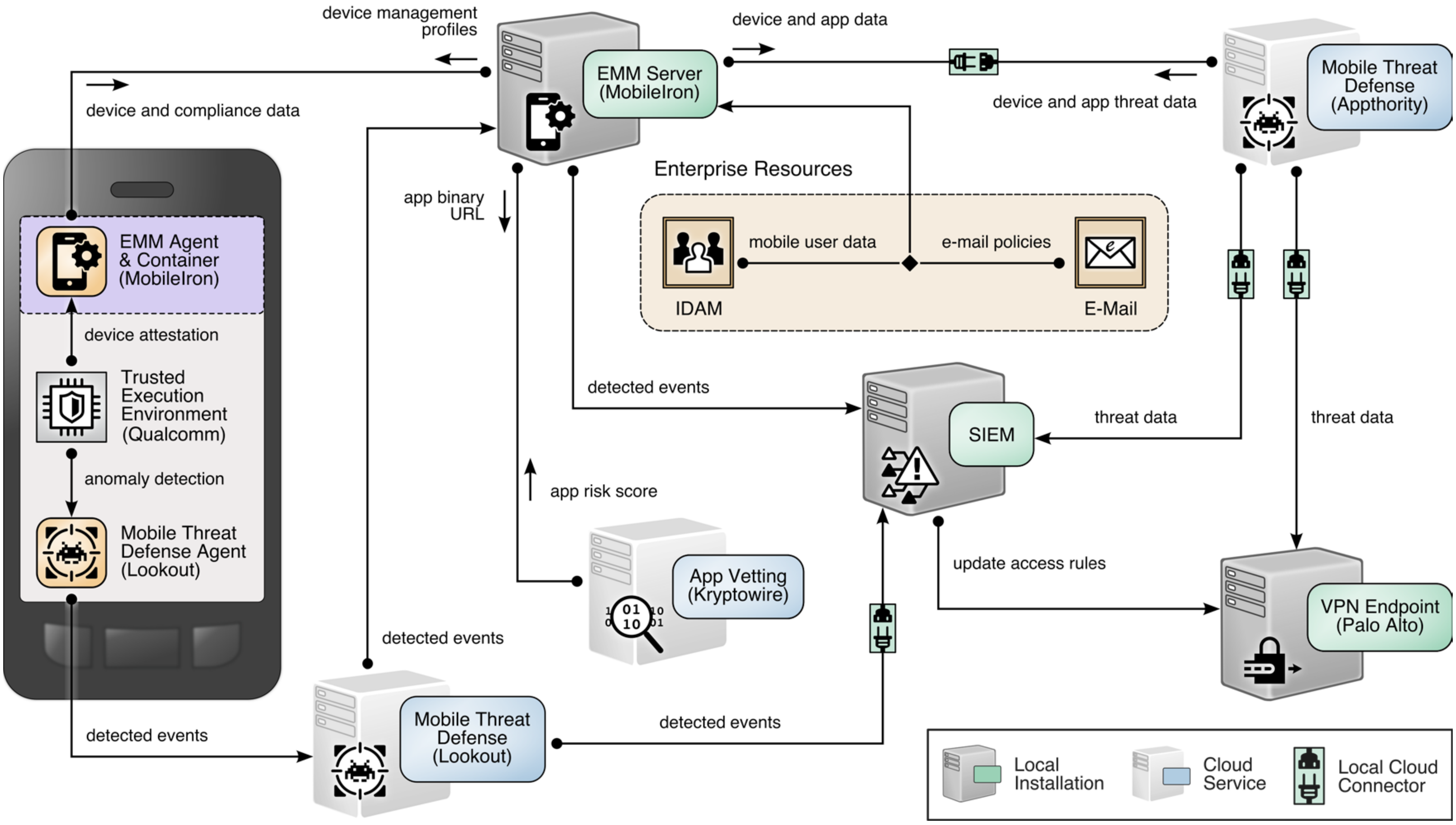
QUALCOMM®

Lookout

kryptowire

apthority

MOBILE DEVICE SECURITY ENTERPRISE (MDSE)



Conclusions

- NIST has an active mobile security portfolio
- Working with great partners:
  - GSA, DHS, etc.
- There is still much to be done
- Standards and guidelines are being updated
- Feedback and participate from the greater community is necessary

CONTACT INFORMATION

Gema Howell

Gema.Howell@nist.gov

https://nccoe.nist.gov

(301)-975-6299