Overview of DISA's T&E Approach for Mobility:

From Devices to Applications

7 May 2012

V3.2

DoD Mobility Overview

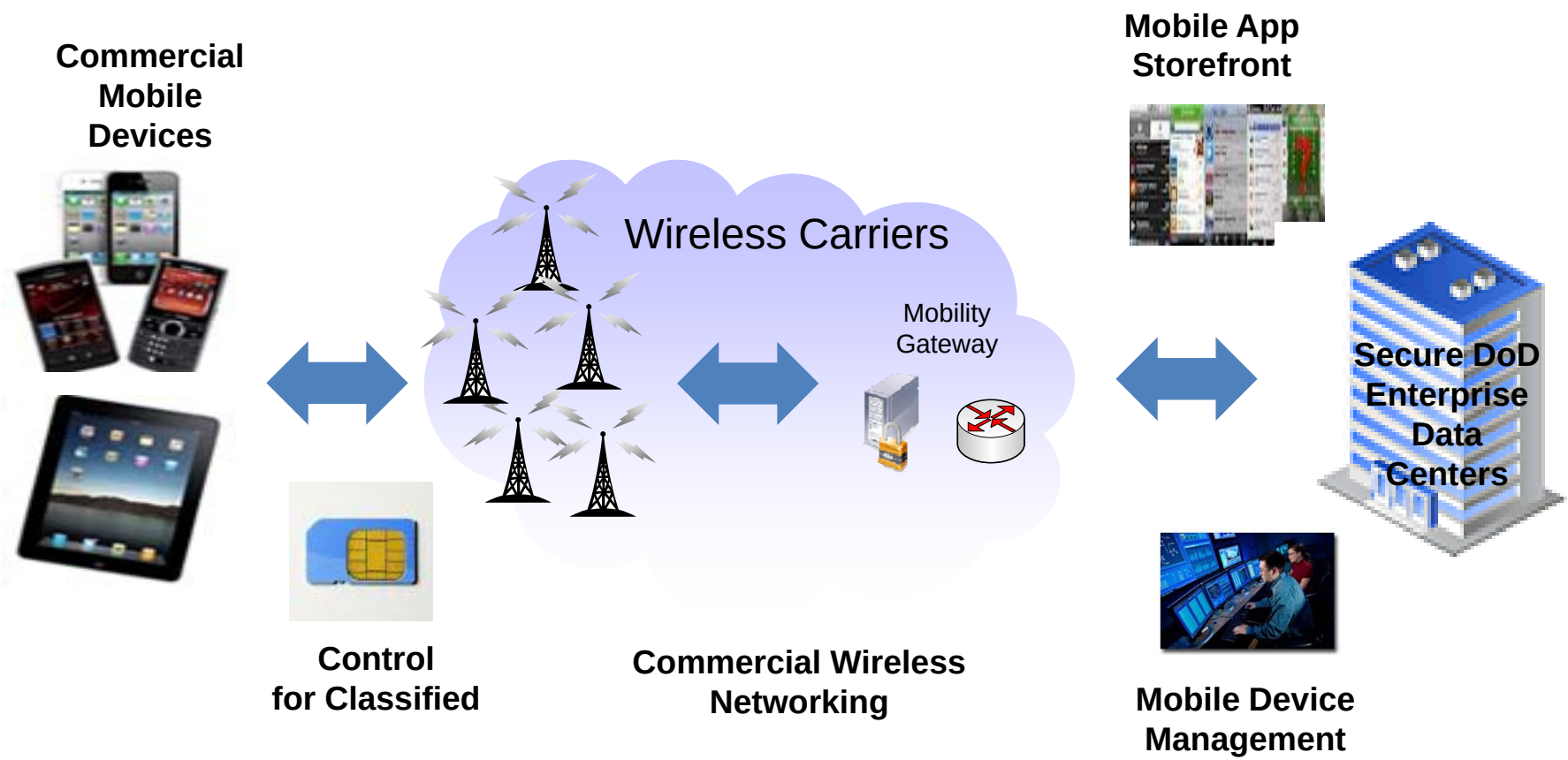
- DoD's Enterprise Mobility Strategy is based on leveraging the Commercial Mobility Services to the maximum extent possible
- Provides access to mobile applications which fit into two categories - standalone applications and enterprise applications
  - Standalone applications will reside in the device and do not interface with external systems
  - Conversely, enterprise applications are built to perform resource-intensive transactions
- Requires connections to Commercial Carriers networks
  - Segment DoD Traffic by using a DoD Virtual Private Network
  - Manage devices to ensure security of enterprise is not compromised
  - Forward carrier network, system performance Situational Awareness data to the prescribed Defense Computing Center

DoD Mobility - Potential Providers

Feature	Blackberry	IOS	Android	Windows Mobile	Windows Phone	Symbian	Maemo	MeeGo	Bada
Manufact-urer	RIM	Apple	Open handset (Google)	Microsoft	Microsoft	Symbian foundation	Nokia	Linux	Samsung
OS Family	Mobile OS	Mac OSX	Linux	Windows CE 5.2	Windows 7	Mobile OS	Linux	Linux	Linux

There are 30+ global smartphone vendors and more than 10 mobile OS platforms; The top four (Apple, Android, RIM and Symbian) control 89% of the total market.

DoD Mobility Overview



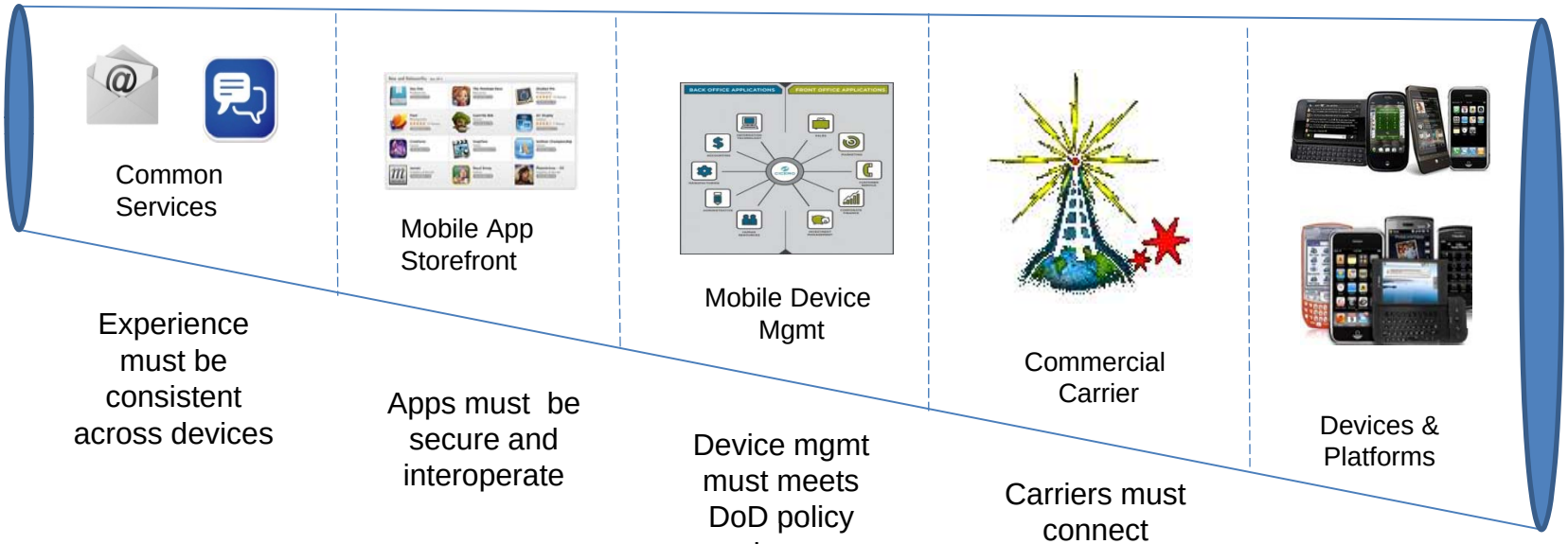
The Mobility Program enables the mobile User and business access to secure government enterprise services.

DISA Mobility T&E Strategy

- Leverage and automate APL testing to ensure devices and platforms meet DoD mobility requirements
- Adapt and evolve Service and Agency application testing programs to support DoD Mobility Application Storefront
- Establish and provide reference implementation and test capability to verify commercial carrier implementations for DoD mobility
- Employ live and virtual devices to verify DoD mobility infrastructure and validate DoD and Carrier mobility management
- Ensure DISA common user and real-time services are tested to the mobility edge

DISA Mobility T&E

Must ensure enterprise solutions are tested to the mobility edge



Experience must be consistent across devices

Apps must be secure and interoperate

Device mgmt must meets DoD policy requirements

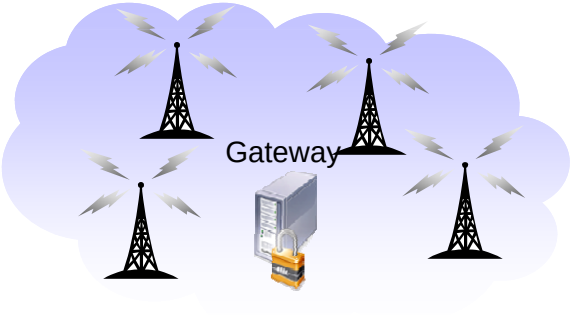
Carriers must connect and perform IAW DISA standards

Devices must meet UC/APL requirements

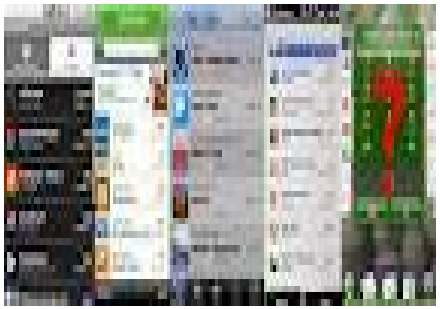
DISA Mobility T&E Components

APL Certified DoD Mobile DEVICES

Certified Wireless Carriers



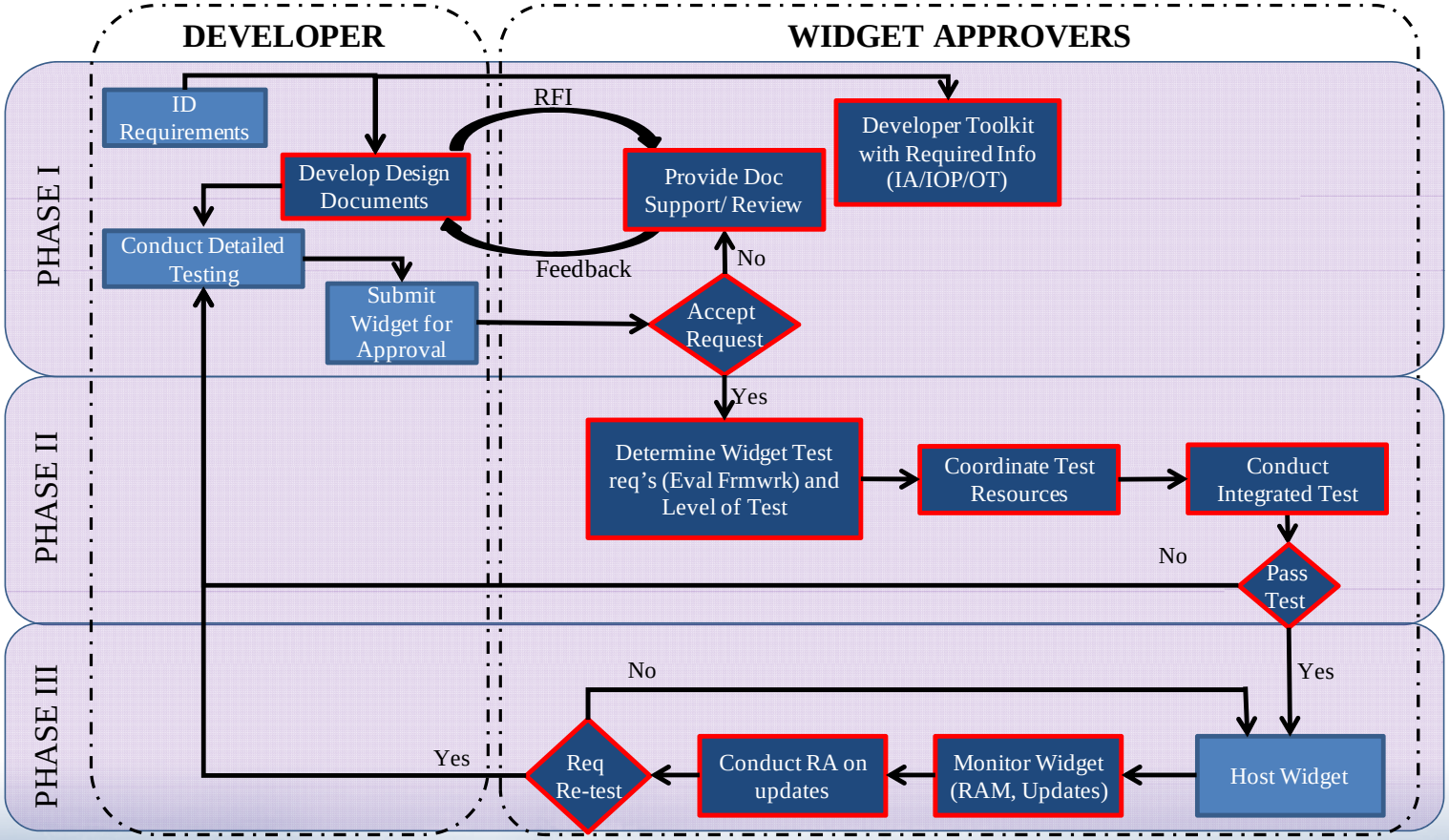
APL Certified DoD Mobile APPS



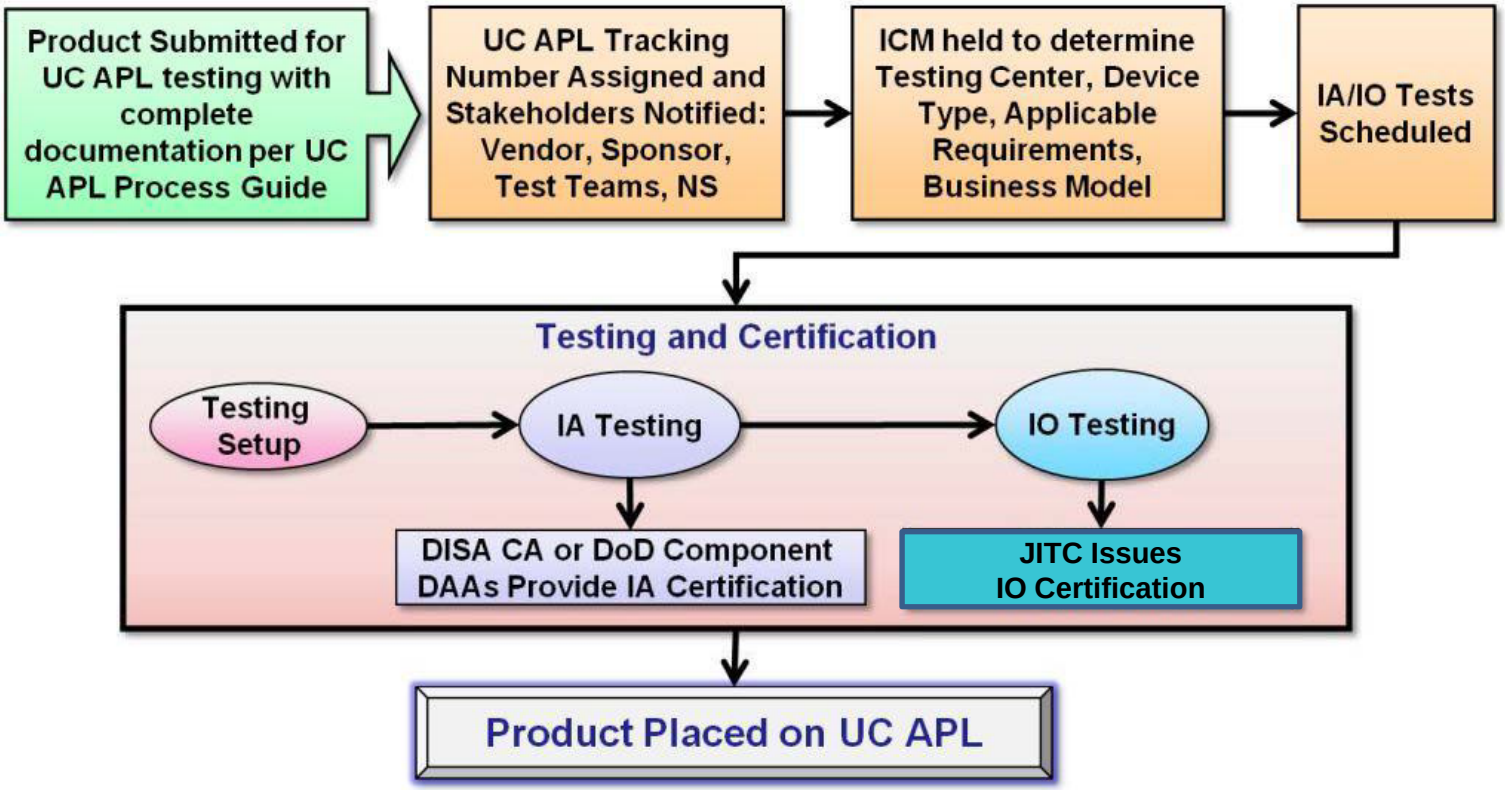
Common User Services T&E

Mobile Device Mgmt T&E

DoD Mobility T&E - Notional Draft Apps Approval Process



DoD Mobility T&E
Draft Device/Platform Approval Process



DISA Mobility T&E Proof of Concept

Apr – Sep FY12

1.5K Android / iOS Devices

- Pre-Loaded APPS
- GOOD Enterprise Email
- DISN VoIP
- Initial MDM/MBSS

Define Device & App Cert Process

Define T&E Environment

Capability & Limitations

Oct – May FY13

6.5K Android / iOS Devices

- Initial MAS -10 APPS
- GOOD Enterprise Email
- DISN VoIP
- MDM/MBSS

Pilot Device & App Cert Process

Stand up T&E environment

Test MDM and E2E Capability

May FY13 ->

10K Android / iOS Devices

- MAS
- Enterprise Email
- DISN VoIP
- MDM/MBSS

Certify Devices and Apps Cert

Test MDM Updates

Test Common Users Services

DISA Mobility T&E Environment

Data collection via embedded agents

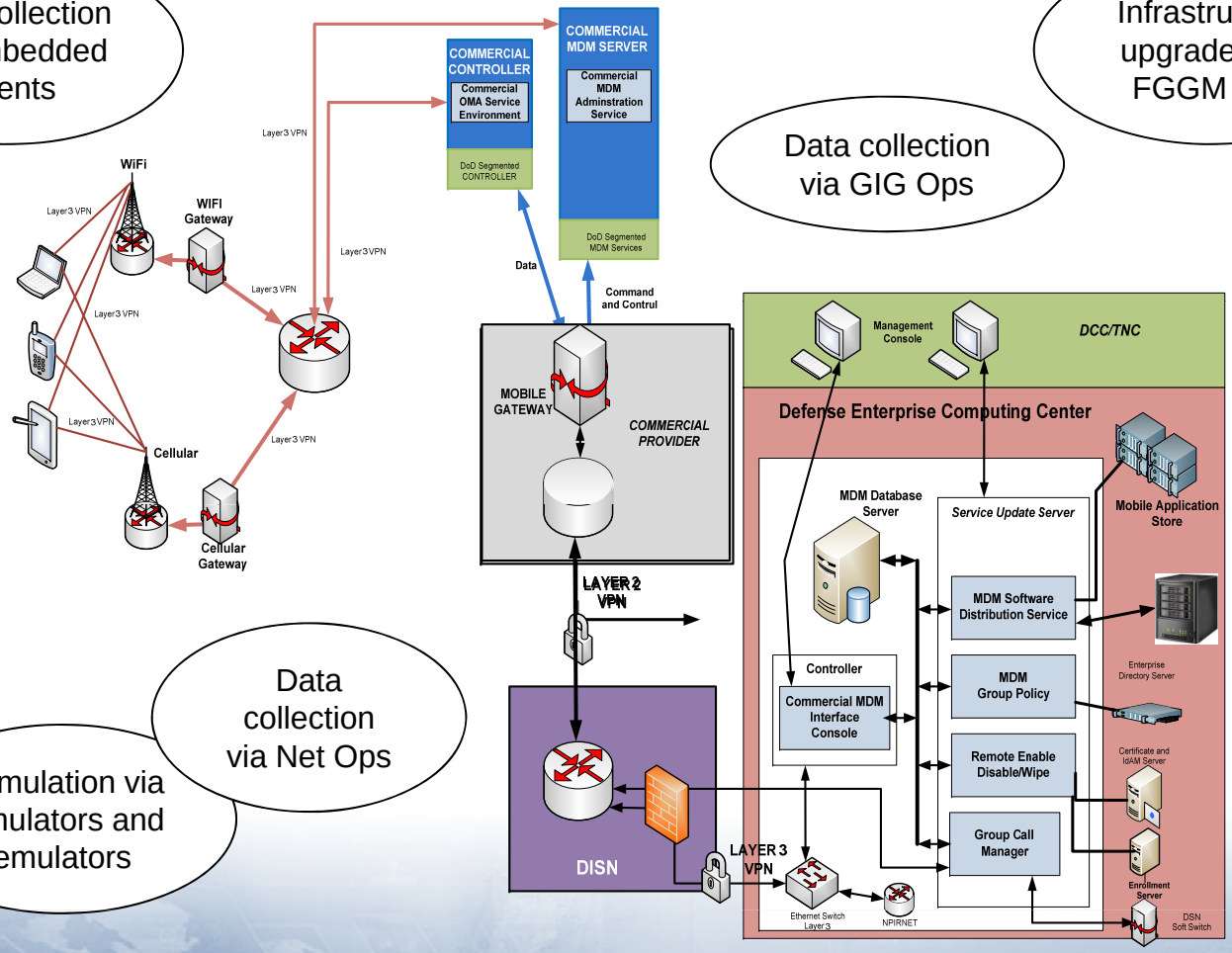
Infrastructure upgrades via FGGM Lab

Data collection via GIG Ops

Application promotion via staging environment

Data collection via Net Ops

Stimulation via simulators and emulators



Summary - DISA Mobility T&E Challenges

- # of mobile device applications, vendors and platforms (configuration management of RIs, scripts, results, certs)
- Applications working on disparate devices
- Use of automation (management and deployment of emulators and simulators)
- Incorporate crowd sourcing test methods (increasing confidence)
- Preserving enterprise level security (policy and management)
- Incorporating mobility into common service T&E (ensuring enterprise services work as expected for deployed users)

DISA
A Combat Support Agency

Questions?