Agile Test and Evaluation (T&E) for converged network services

- Unified Capabilities -

Mr. Richard Delgado Jr.
richard.delgado.civ@mail.mil

6 November 2012

Version 2.0

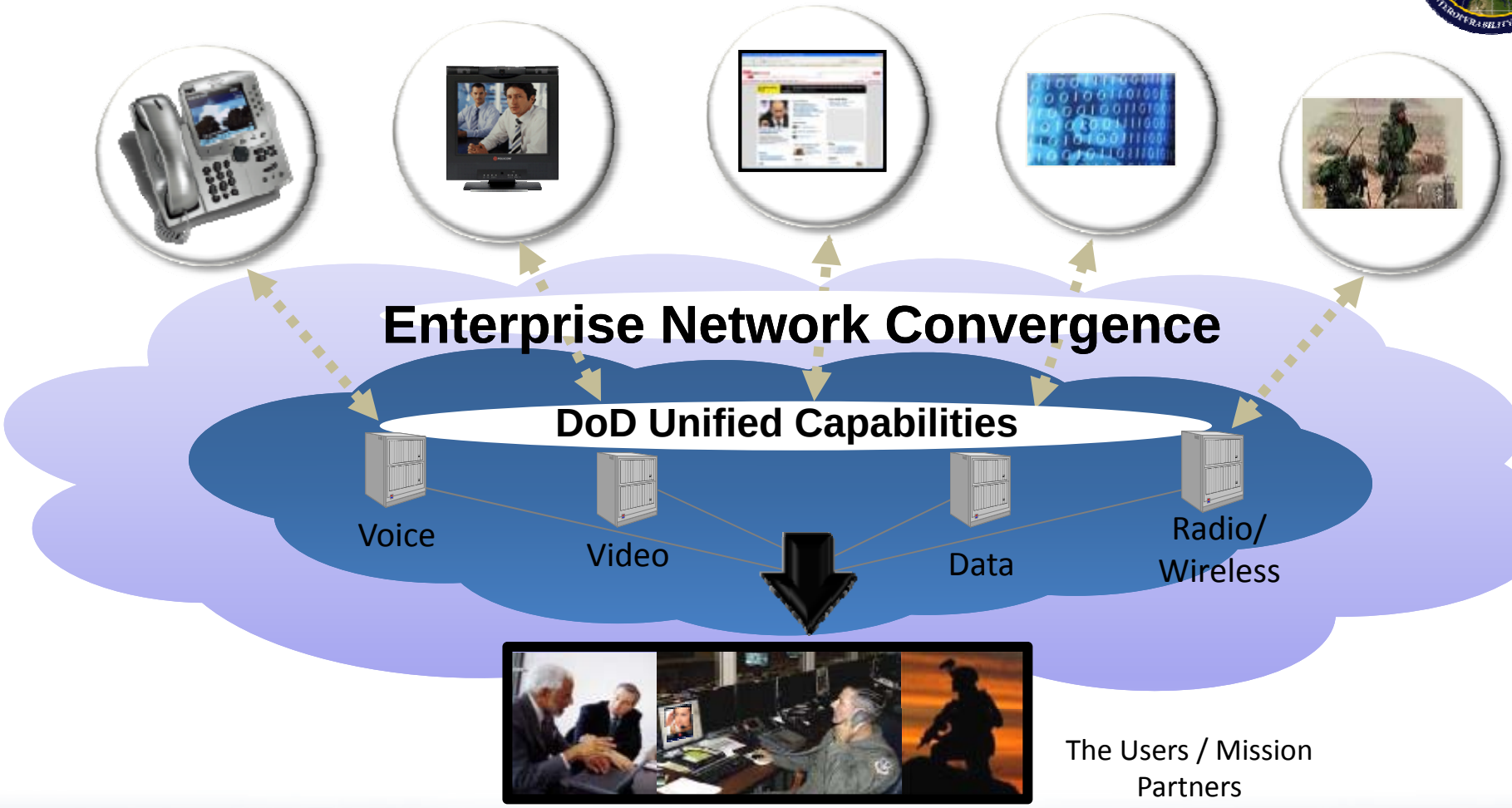
Disclaimer

- **The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.**

Agenda

- **UCR Overview:**
  - Converged IP Services
  - UC Policy and Directives
  - UCR and the UC APL
  - Agile Testing
  - UC Distributed Testing
  - Way Ahead

DISA Information Technology (IT) Enterprise Target State (Convergence)



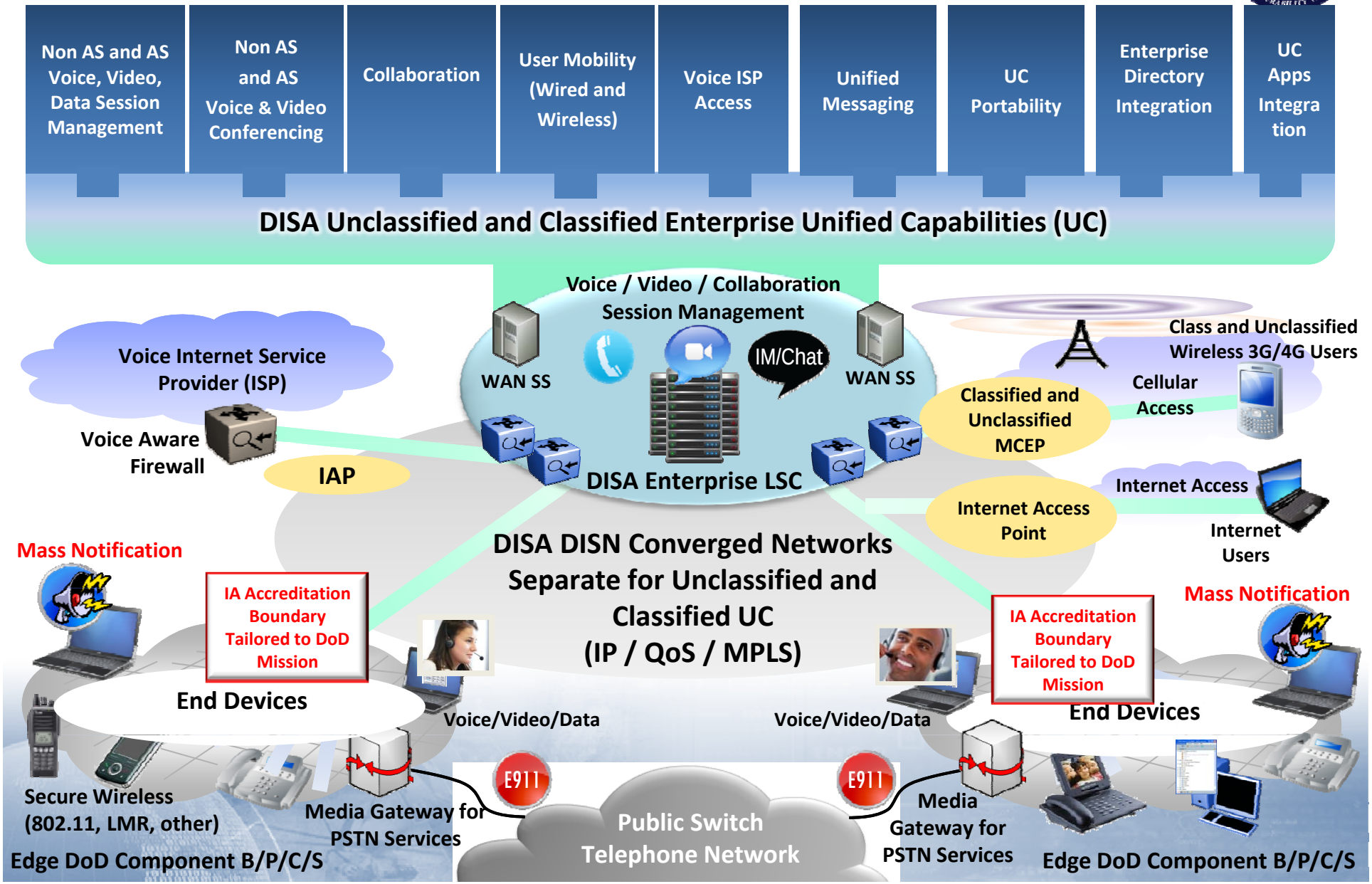
The Users / Mission Partners

Interoperability → Information Assurance → Network Performance

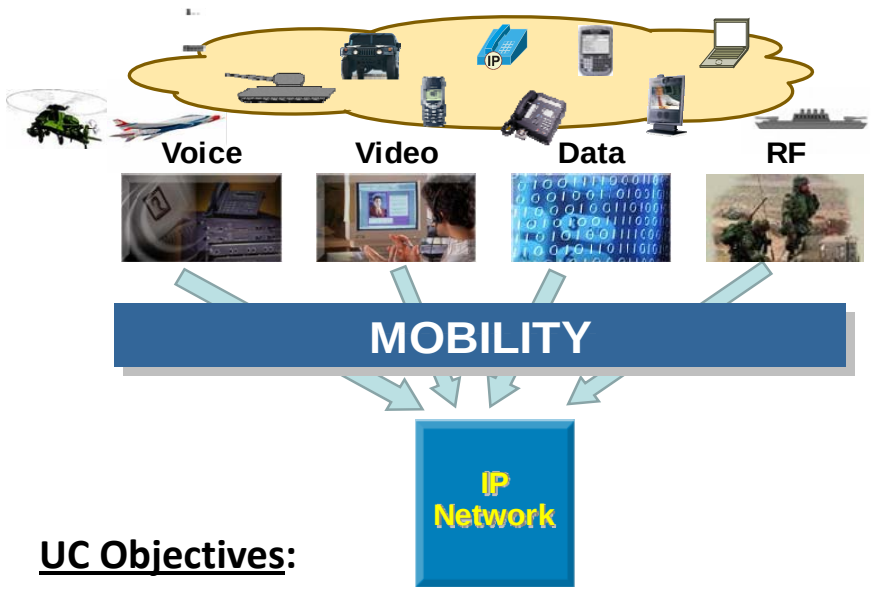
Robust, diverse and resilient protected communications, and computing environment

Leading the Migration to Almost Every Thing Over IP (EoIP)
Multi-vendor Environment, Enabling Net-Centric Operations

CAPABILITIES VIEW-1, VISION



DoD Unified Capabilities (UC)



UC Objectives:

Migrate DoD to common, converged IP-based network services to achieve:

- Integrated and interoperable operations
- End-to-end security
- Shared situational awareness
- Enhanced wireless and mobility support
- Improved support for communications on the move
- Real-time collaboration (integrated voice, video, and/or data services)

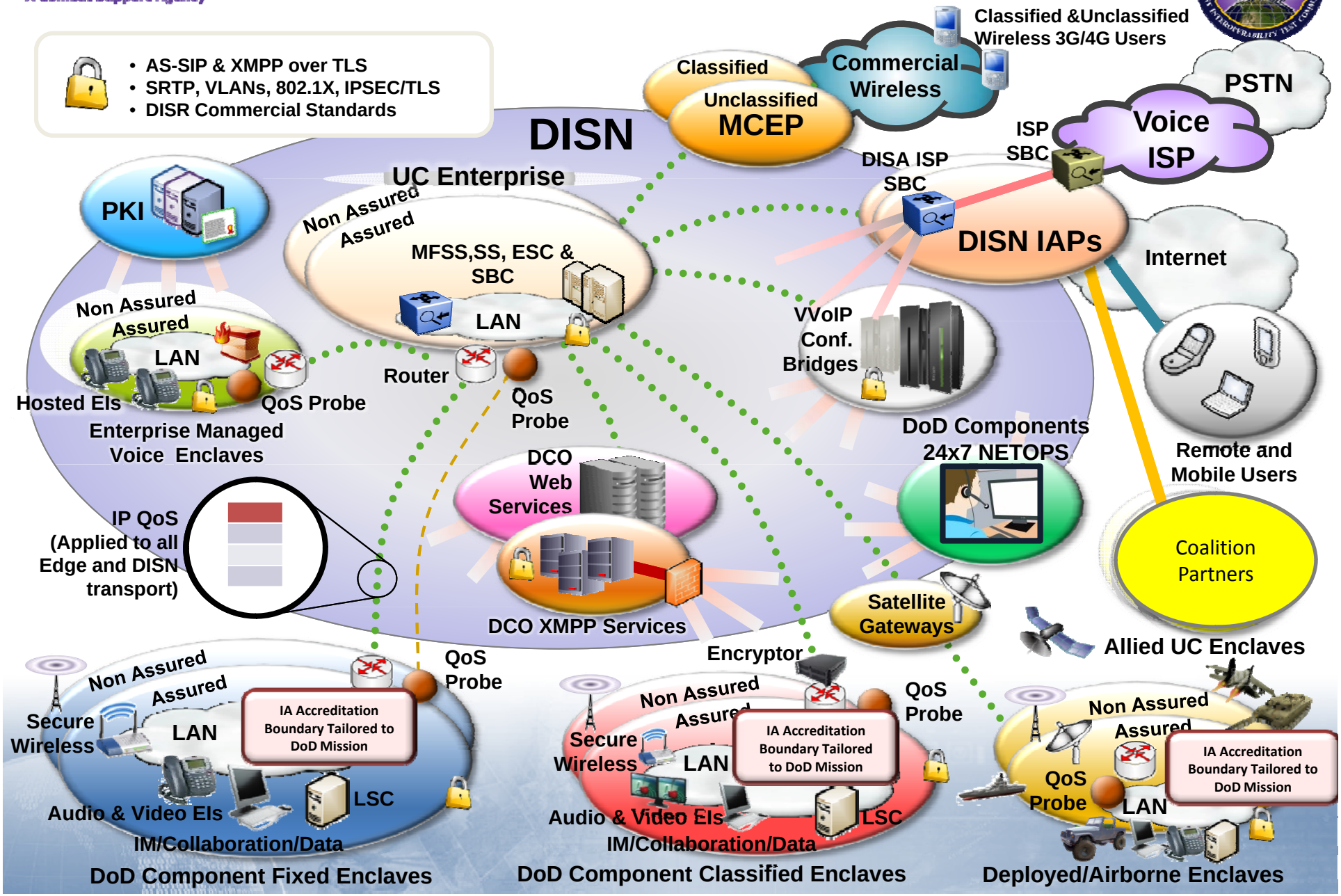
UC Definition:

The integration of voice, video, and/or data services delivered ubiquitously across an interoperable, secure, and highly available IP network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter

UC Tenets:

- Leverage commercial off-the-shelf technology to meet DoD's mission requirements
- Accelerate migration of increasingly costly legacy circuit switch technologies to interoperable and secure IP-based net-centric services
- Standardize and consolidate Component IP convergence efforts across DoD to reduce telecommunications costs and streamline management
- Achieve savings by implementing enterprise requirements for interoperability, security, and network performance
- Implement competitive acquisitions of approved products, based on common user requirements

Unified Capabilities Reference Architecture



UC Governing Documents

DoD CIO

- DoD CIO IT Enterprise Strategy and Roadmap
- DoDI 8100.04
- Unified Capabilities Requirements (UCR)
- Unified Capabilities Master Plan (UC MP)

Joint Staff Implementation Guidance

- CJCSI's Implementing UC

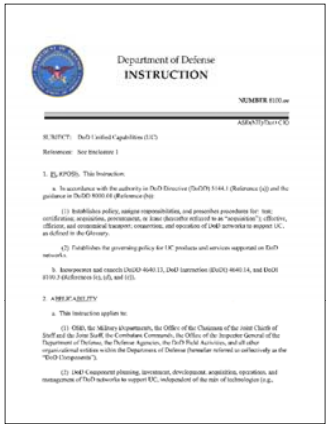
DISA Planning

- DISA Campaign Plan
- DISA GIG Convergence Master Plan
- DISN Technical Evolution Plan

DoD Component Network Implementation

- UC Implementation Plans
- UC Network Cutover Plans

DoDI 8100.04 (9 Dec 2010)



Department of Defense
INSTRUCTION

NUMBER 8100.04

ASD(NII)/DoD CIO

SUBJECT: DoD Unified Capabilities (UC)

Reference: See Enclosure 1

1. PURPOSE. This Instruction:

a. In accordance with the authority in DoD Directive (DoDD) 5144.1 (Reference (a)) and the guidance in DoDD 8000.01 (Reference (b)):

(1) Establishes policy, assigns responsibilities, and prescribes procedures for: test; certification; acquisition, procurement, or lease; effective, efficient, and economical transport; connection; and operation of DoD networks to support UC, as defined in the Glossary.

(2) Establishes the governing policy for UC products and services supported on DoD networks.

b. Incorporates and cancels DoDD 4640.13, DoD Instruction (DoDI) 4640.14, and DoDI 8100.3 (References (c), (d), and (e)).

2. APPLICABILITY

a. This Instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

(2) DoD Component planning, investment, development, acquisition, operations, and management of DoD networks to support UC, independent of the mix of technologies (e.g.,

Purpose:

Establishes policy, assigns responsibilities, and prescribes procedures for: test; certification; acquisition, procurement, or lease; effective, efficient, and economical transport; connection; and operation of DoD networks to support UC

Applicability:

- All DoD Components
- DoD Component planning, investment, development, acquisition, operations, and management of DoD networks to support UC, independent of the mix of technologies, and whether converged or non-converged
- UC support for authorized non-DoD users (e.g., combined or coalition partners and U.S. Government departments and agencies)
- Acquisition of services as described in DoDD 5000.01 and DoDI 5000.02

Policy:

- DoD Components integrate current network technologies with future network technologies to provide UC
- DoD Components comply with functional requirements, performance objectives, and technical specifications for DoD networks that support UC, as specified in the DoD Unified Capabilities Requirements (UCR)
- Products that provide or support UC, acquired or operated by the DoD Components, shall be certified for interoperability and Information Assurance (IA)
- DoD networks support UC during all phases of DoD operations
- DISA is the preferred UC transport provider for Internet and commercial satellite connections used for voice, video, and/or data services on DoD networks

UC Master Plan

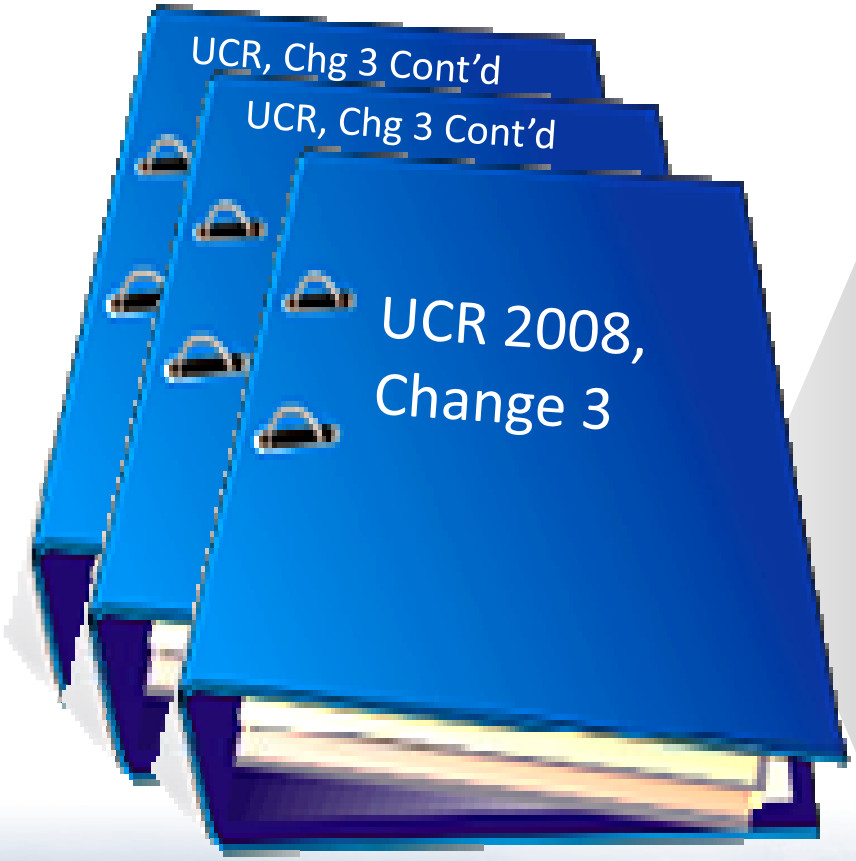
- **Defines the implementation strategy to achieve IP Convergence**
  - **Guides DOD Components in planning, investments, acquisition, Operations and Maintenance, sustainment, and Program Objective Memorandum submissions**
  - **Identifies Reference Architectures for UC Implementation. Provides various AV, OV, CV, SV artifacts**
  - **Guides the resource planning, Business Case Analysis, and investment strategy for FY12-16**
- **Coordinated through the UC Steering Group with Senior Leadership (GS-15 equivalent) from Services and Agencies**

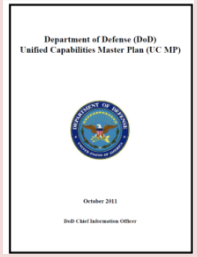
UC Requirements

- **Establish standards to develop unified capability solutions.**
  - **Identifies only the MINIMUM requirements and features to support UC Reference Architecture**
  - **Does not contain a complete set of specifications for COTS features that <u>do not</u> affect assured services**
- **UCR 2008 (CH3) is the current approved version. UCR 2013 in Draft.**
- **Allows for standardized Unified Capability Test Plans (UCTPs) for Interoperability (IO) and Information Assurance (IA) testing.**
- **Facilitates collaborative development of Information Support Plans (ISPs)**
  - **I.E., for programs under traditional acquisition requirements (CSI 6212.01E)**

UC Requirements are Minimum Essential

UCR 2013 Restructure





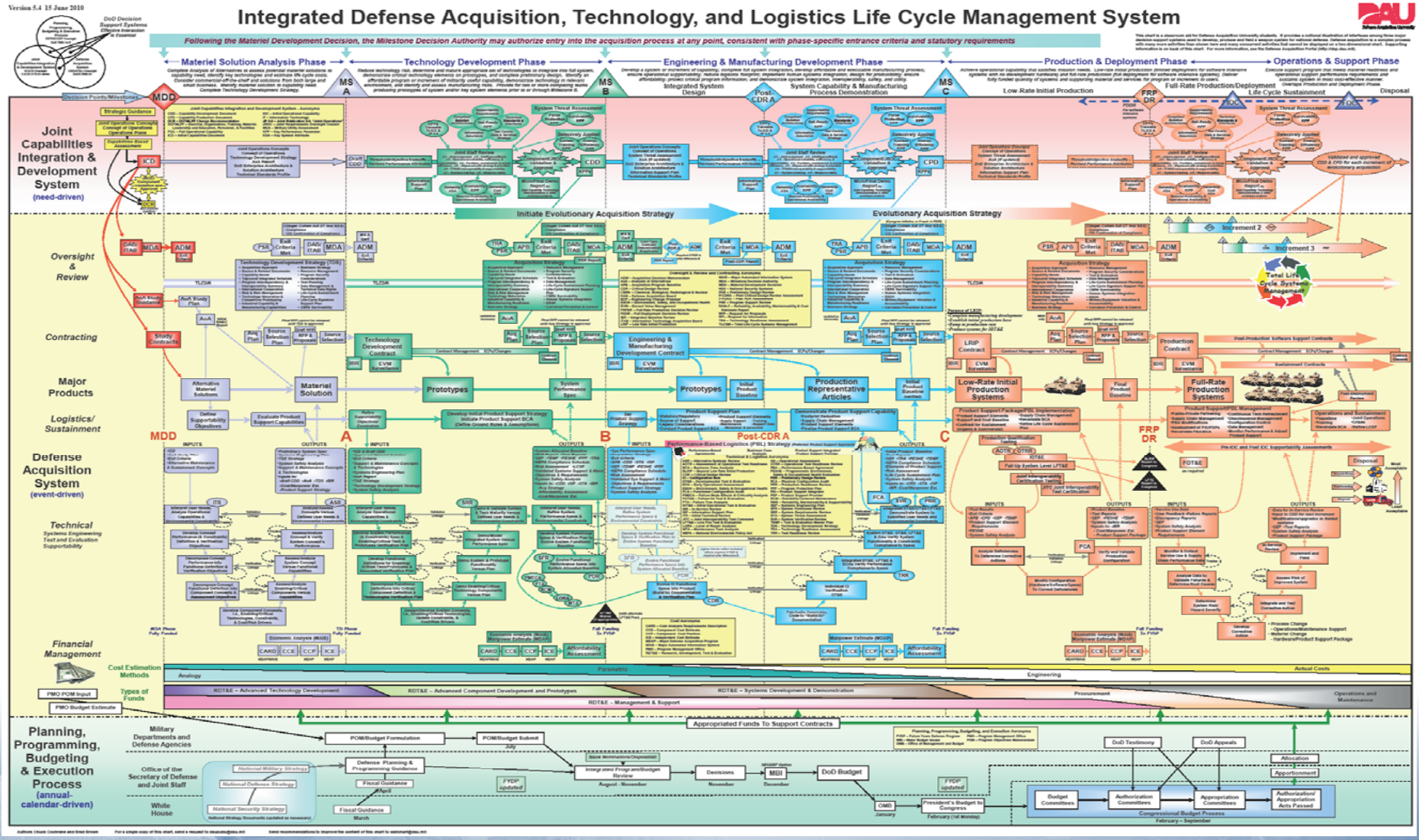
Department of Defense
INSTRUCTION
8100.04

CJCSI 6211.02D

UC 2013 Specifications

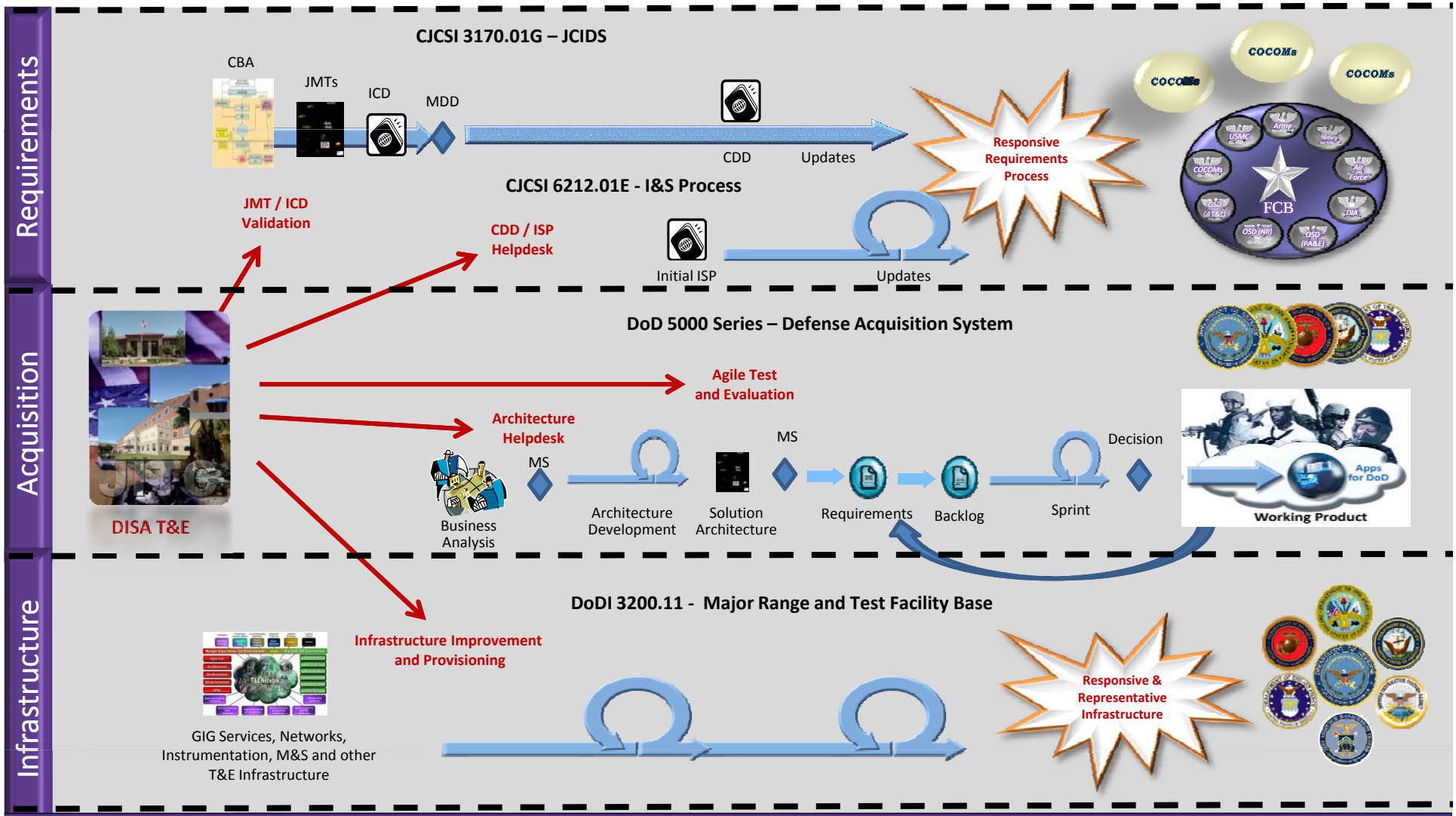
- **Remove IPv6 Profile**
- Remove SS7 Gateway Req

Acquisition Today



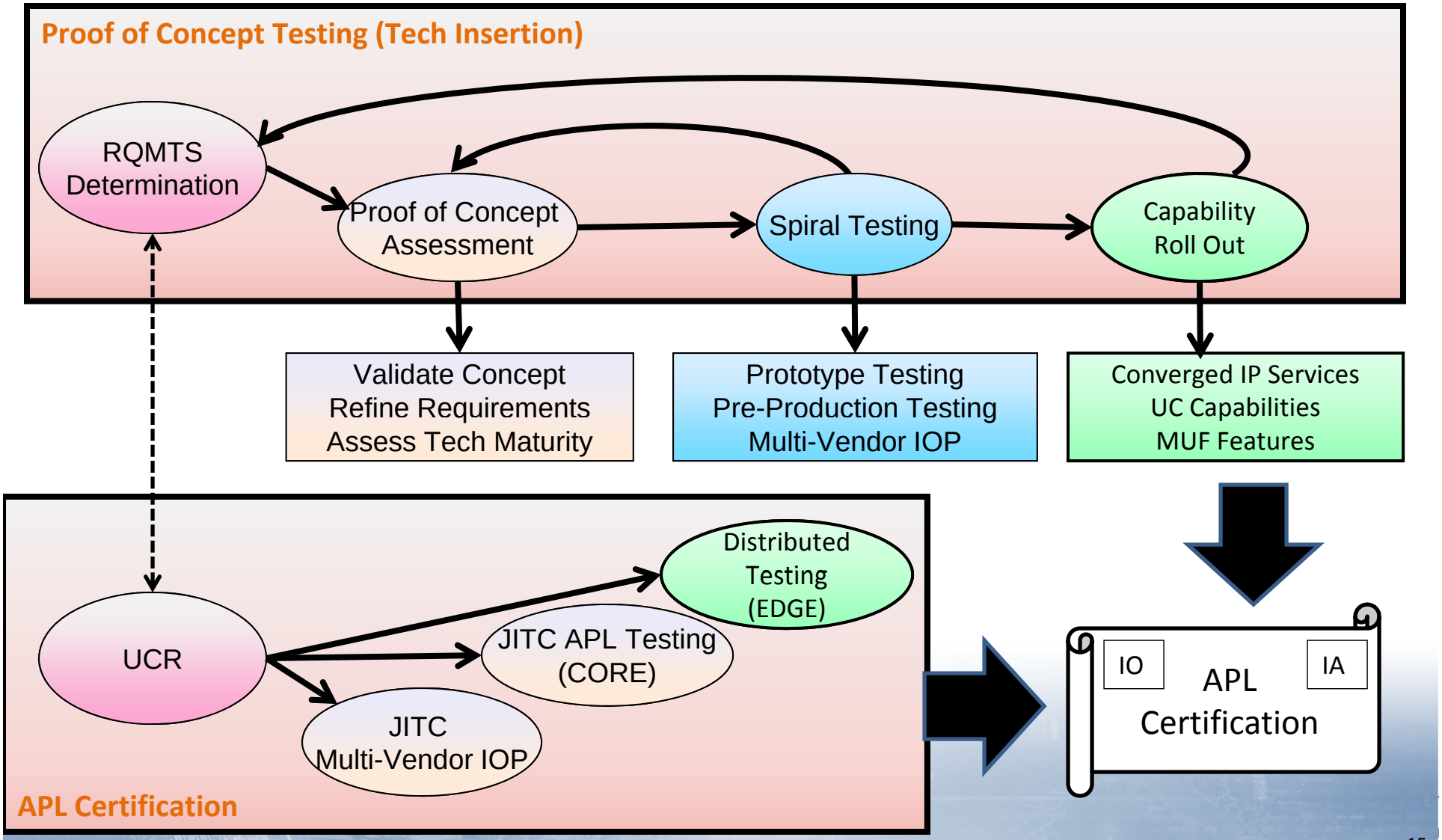
Moving DoD IT Acquisition Forward

Provisioning integrated services across acquisition processes and life-cycle



Making Acquisition Processes and Infrastructure Responsive to the Warfighter

UC Product Support



UC Distributed Testing
"Test Once, For Many"

- **Single UC APL for use by the DOD CIO and DOD Components in acquisition and procurement**
- **Effectively integrates MILDEP labs and industry into the T&E Process**
- **There shall be a DoD Component sponsor for each vendor product**
- **JITC is sole Interoperability Certifier for UC APL**
  - **Distributed testing based on common requirements and common test plans (UCR 2008 and the JITC UC TP)**
  - **Leverage existing MILDEP capabilities and expertise for "Edge" devices**
- **"Test Once for Many"**
  - **Use all available test resources and data**
  - **Reciprocity among UC Community (IO/IA)**

UC Distributed Testing Precepts

- **UCCO manages the UC Distributed Testing and Certification Process**
  - **Scheduling, vendor interface, test status, test results, UC APL posting and maintenance, UCR coordination, IO/IA adjudication**
- **Established UC Rules of Engagement**
  - **Determine Lab Capabilities (infrastructure, procedures, etc.)**
  - **Develop Business Model for Fee For Service**
  - **Integrate MILDEP labs into UCCO/APL process**

Distributed Testing ROEs
Where to Test?

- **Distributed Test Working Group - DISA NS, DISA Service Managers, JITC, Army ISEC-TIC, Air Force TSSAP, Navy SPAWAR**
- **Based on Lab Capabilities**
  - **Infrastructure to test requirements of a product category**
  - **Expertise/training**
- **Based on Availability**
  - **First right of refusal**
  - **Schedule**
- **Based on funding model**
  - **Vendor Fee for Service**
  - **CRADA**

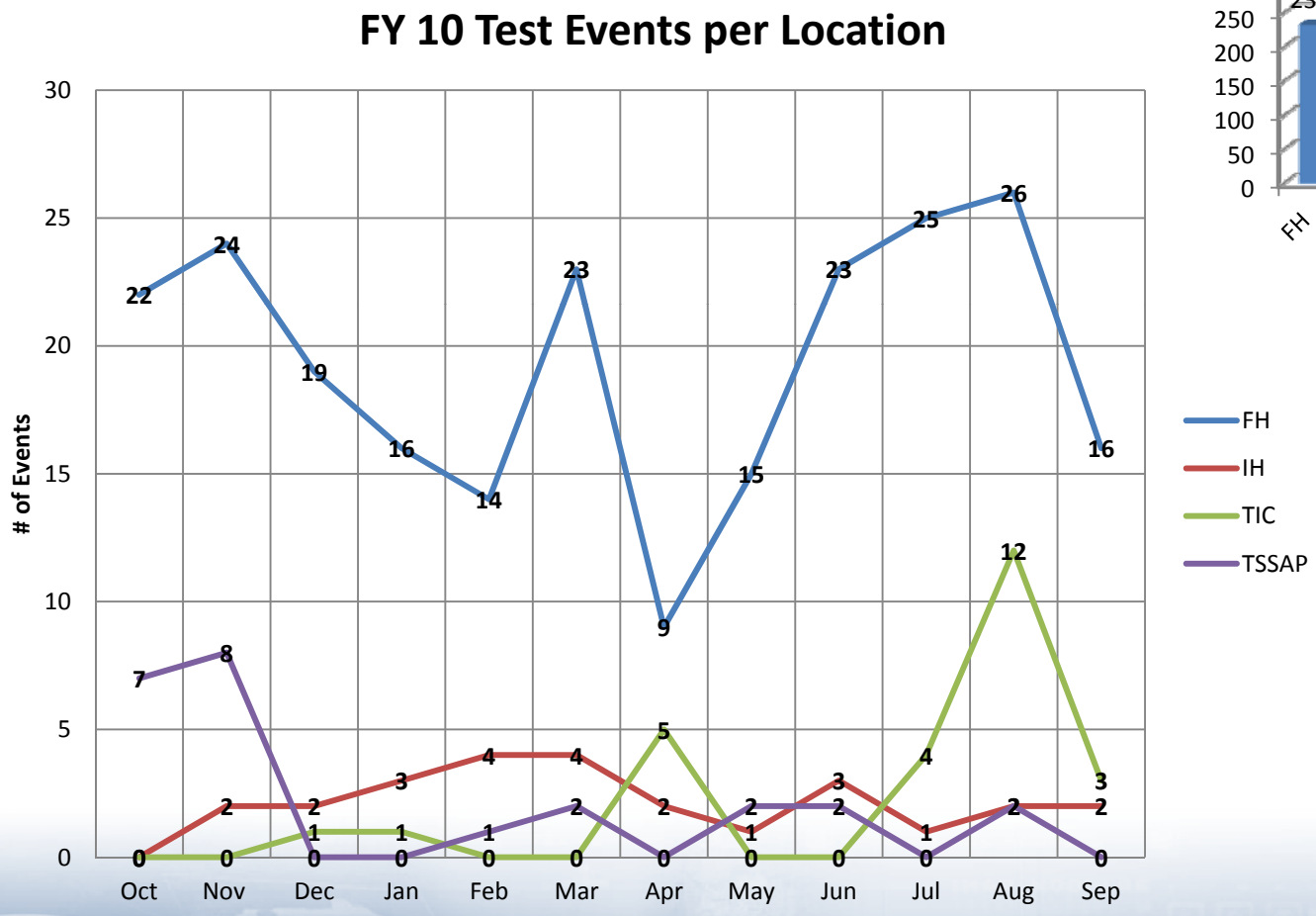
Distributed Testing
What to Test?

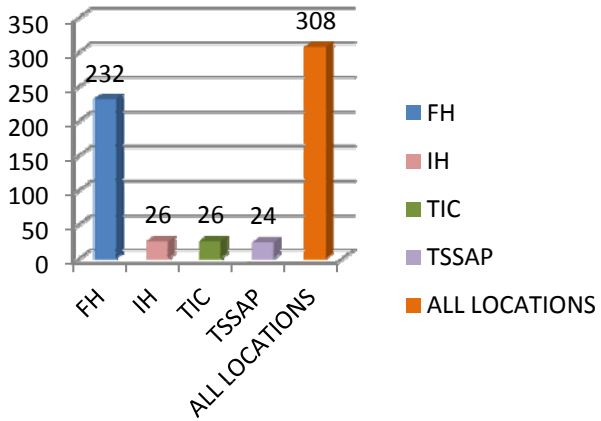
Technical Maturity Matrix

Services Complexity	Prototype	Pre-Production	APL Ready	Post APL
ASFs	• Full test • Or incremental test and/or desk-top review (DTR) if based on previously tested product	• Full test • Or incremental test and/or DTR if based on previously tested product	• Full test • Or incremental test and/or DTR if based on previously tested product	• Full test for new software versions or significant IA-affecting hardware changes • Or incremental test and/or DTR if based on previously tested product
Non ASFs Affecting ASFs	• Partial test • Full test of interaction of features • Or incremental test and/or DTR if based on previously tested product • No test. Vendor letter of compliance (LOC) of vendor tests of non assured services features meeting brochure claims	• Partial test • Full test of interaction of features • Or incremental test and/or DTR if based on previously tested product • No test. Vendor LOC of vendor tests of non ASFs meeting brochure claims	• Partial test • Full test of interaction of features • Or incremental test and/or DTR if based on previously tested product • No test. Vendor LOC of vendor tests of non ASFs meeting brochure claims	• Partial test • Full test of interaction of features for new software versions or significant IA-affecting hardware changes • Or incremental test and/or DTR if based on previously tested product • No test. Vendor LOC of vendor tests of non ASFs meeting brochure claims
Non ASFs Not Affecting ASFs	• Random test of potential interactions	• Random test of potential interactions	• No test • Vendor LOC of vendor tests of features meeting brochure claims	• No test • Vendor LOC of vendor tests of features meeting brochure claims

UC Trend Analysis

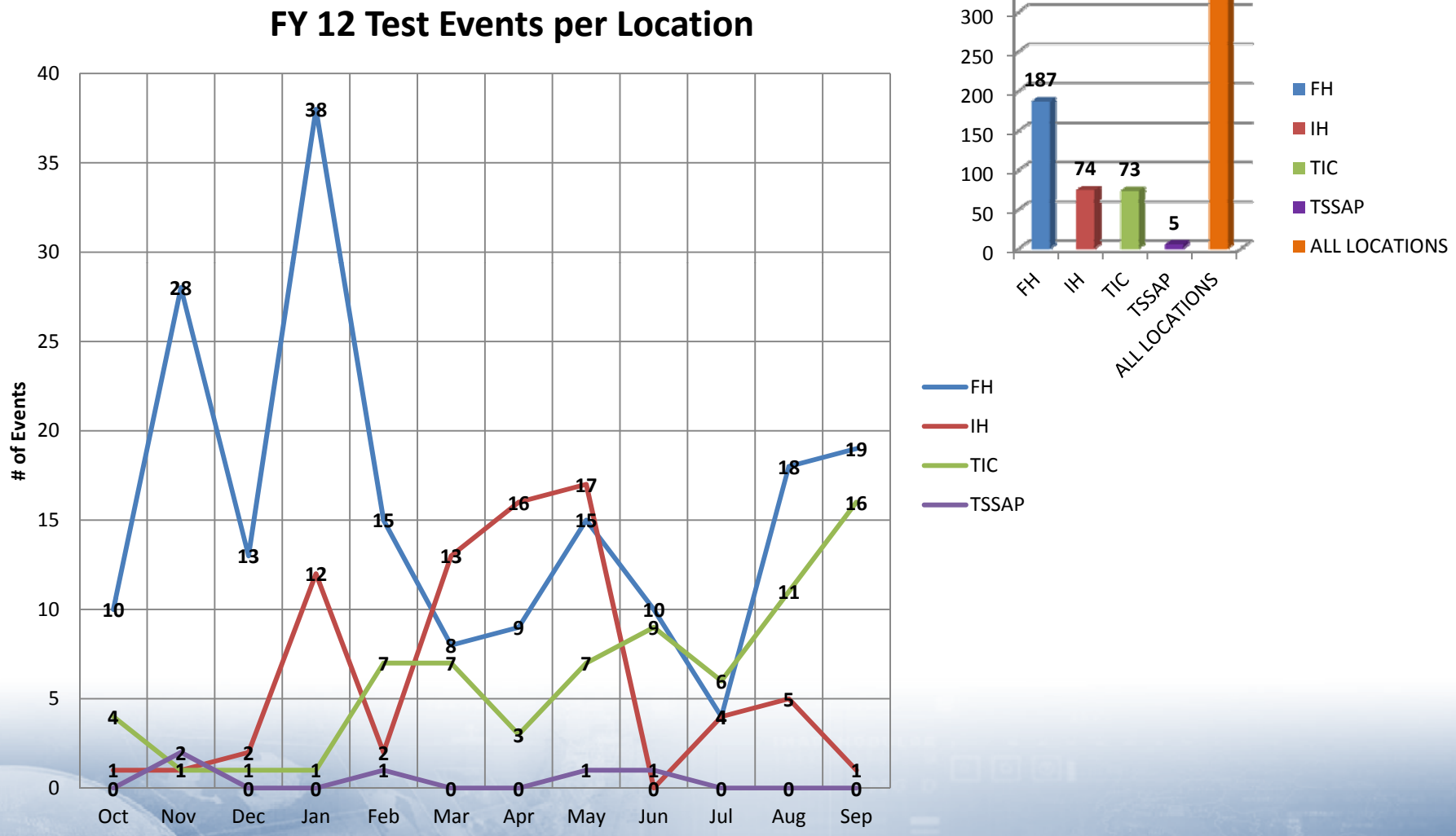
- **FY10 by Location:**



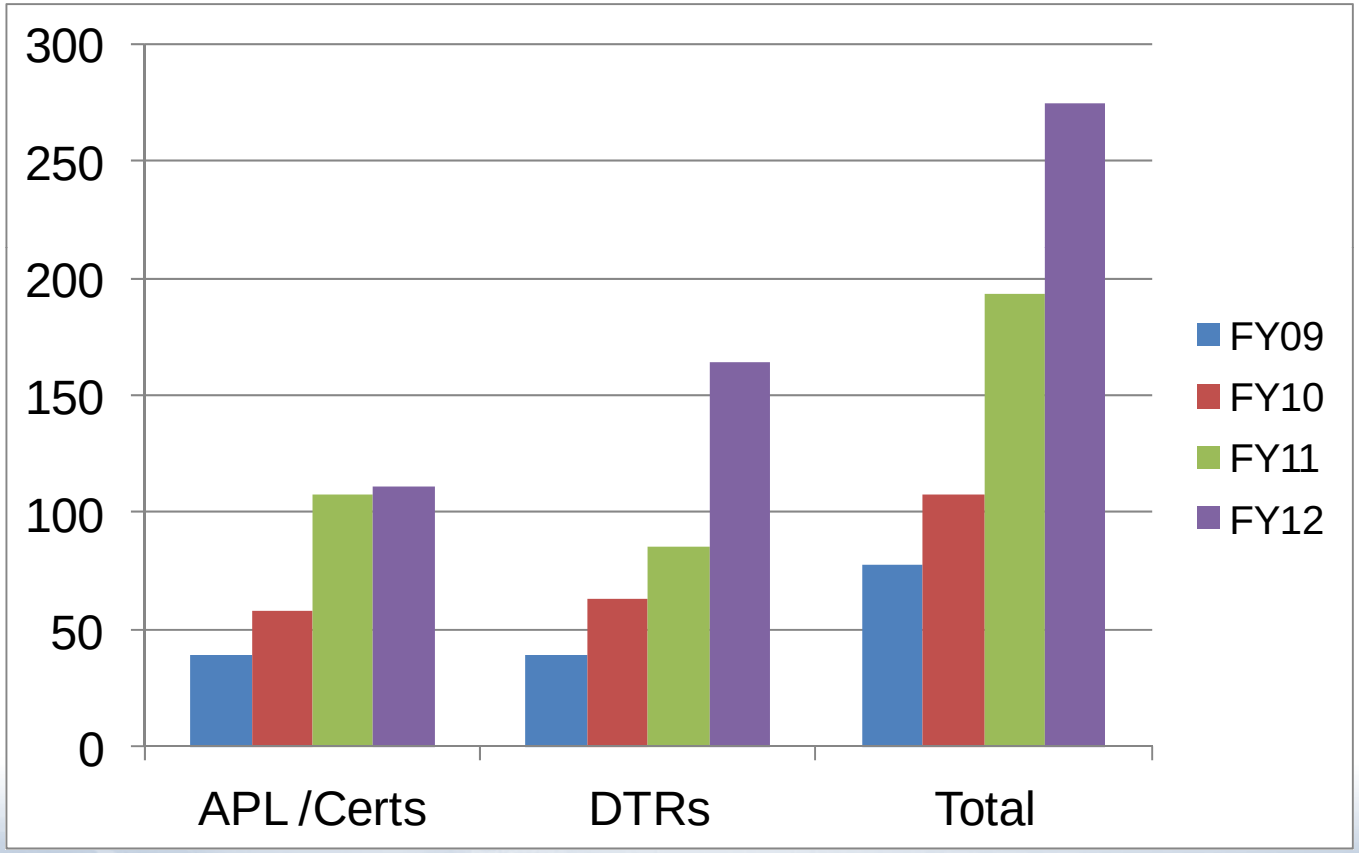


UC Trend Analysis (cont'd)

- **FY12 By Location:**



Summary of UC Events Added to APLITS



Unified Capabilities Way Ahead

- **Continue Deployment of Enterprise Unified Capabilities**
  - **Deployment of WAN SS, LSCs, and Enterprise Voice, Video, and Data Services**
  - **NETOPS integration into DISN OSS Model**
  - **DOD Mobility**
- **UCR Updates (UCR 2013)**
  - **Impacts UC Test Plans and Procedures**
  - **Brings new technology and products into the process**
- **Maturation of Distributed Testing Capabilities**
  - **Federated lab capabilities**
  - **Process improvements to streamline testing and adjudication process**

JITC

Unparalleled Value-Added to the WARFIGHTER

The BATTLEGROUND should never be the TESTING GROUND

BACKUP SLIDES

UCR and UC Framework 2013

Synchronized Table of Contents

UCR 2013

Requirements

1.0 Introduction
2.0 Session Control Product
3.0 Auxiliary Services
4.0 Information Assurance
5.0 IPv6
6.0 Network Infrastructure End-to-End Performance
7.0 Network Edge Infrastructure
8.0 Multifunction Mobile Devices
9.0 Video Distribution System
10.0 Network Infrastructure Product
11.0 Network Element
12.0 Generic Security Device
13.0 Security Devices
14.0 Online Storage Controller
15.0 Enterprise and Network Management Systems
Appendix A Unique Deployed (Tactical)
Appendix B Unique Classified Unified Capability
Appendix C Acronyms

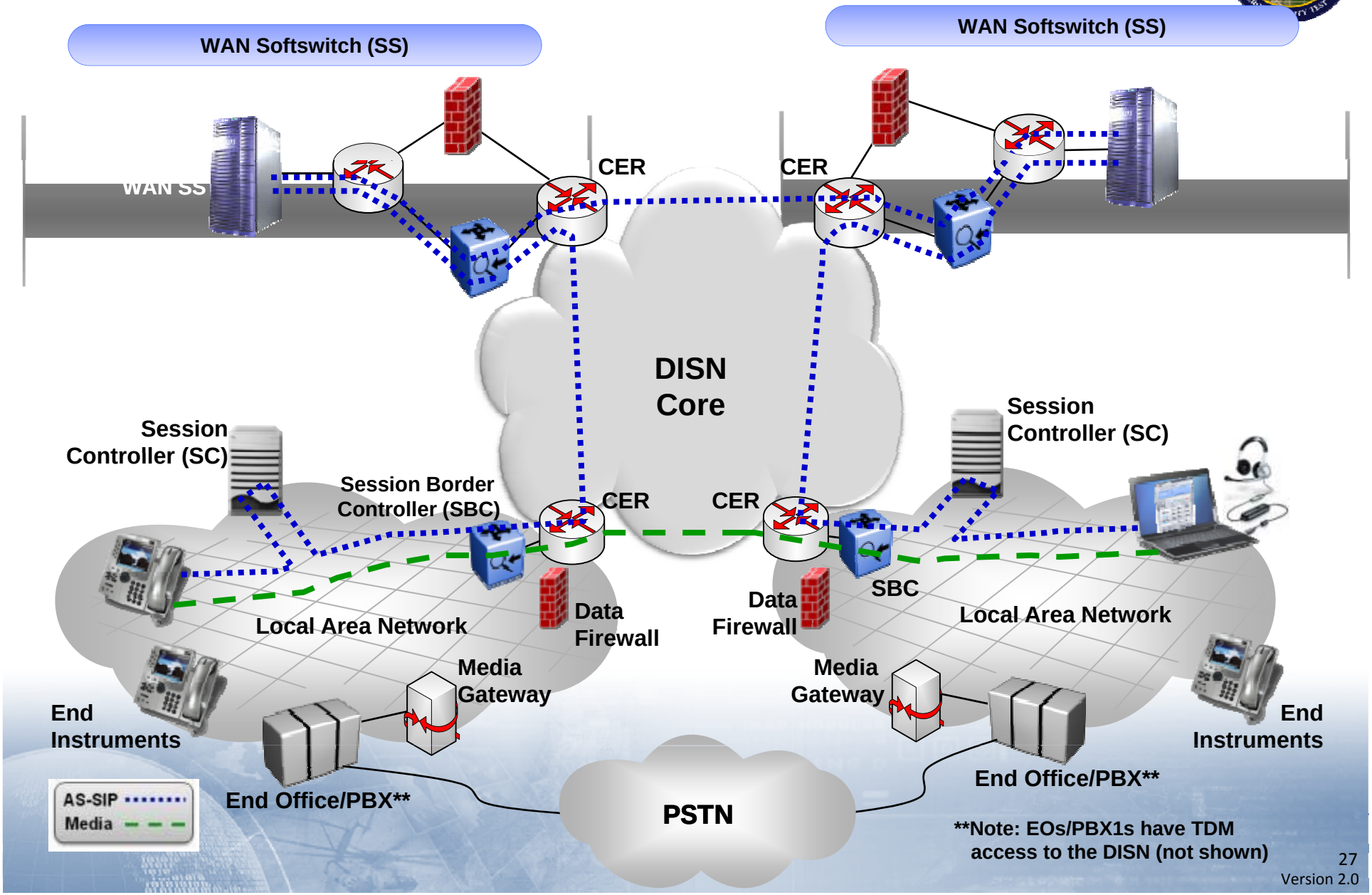
UC Framework 2013

Description and Design

1.0 Introduction and UC Design Overview
2.0 Session Control Product
3.0 Auxiliary Services
4.0 Information Assurance
5.0 IPv6
6.0 Network Infrastructure End-to-End Performance
7.0 Network Edge Infrastructure
8.0 Multifunction Mobile Devices
9.0 Video Distribution System
10.0 Network Infrastructure Products
11.0 Network Elements
12.0 Generic Security Device
13.0 Security Devices
14.0 Online Storage Controller
15.0 Enterprise and Network Management Systems
Appendix A Unique Deployed (Tactical)
Appendix B Unique Classified Unified Capability
Appendix C Def, Abbr, Acronyms, and Ref

UC Distributed Architecture

MILDEP Owned and Managed Session Controller

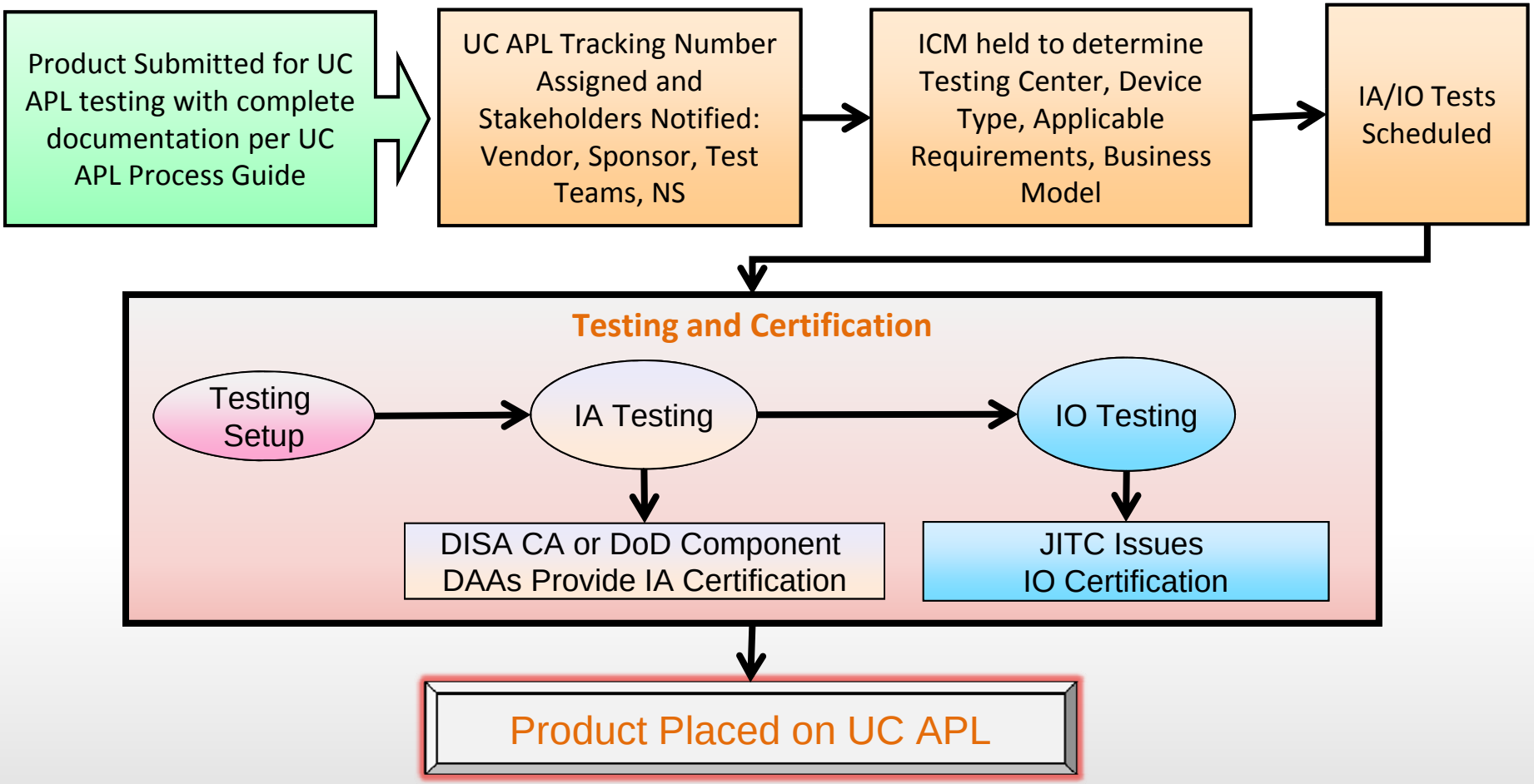


Backbone Deployment Status

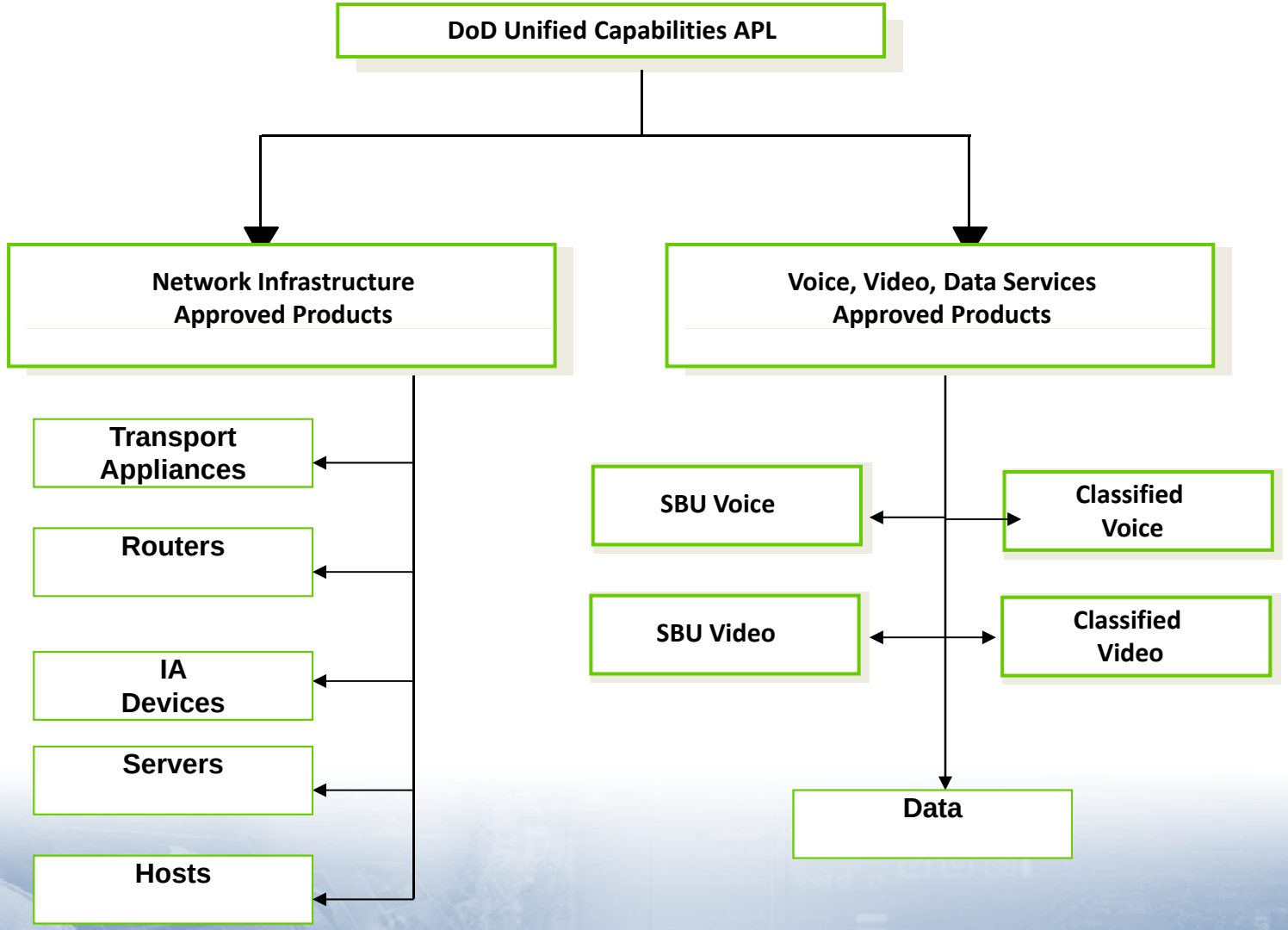
- **DISA Unclassified UC Backbone is FOC as of Jul 2011**
  - Allows MilDeps to connect MilDep operated LSCs to DISA
  - Supports voice and point to point video
- **15 Soft Switches currently active in network of 18 planned**
  - 12 Avaya, 3 Nokia Siemens
  - 3 Avaya installations currently ongoing (Wahiawa, Arifjan, Bahrain)
- **DISA Enterprise Classified Vido/VoIP Backbone is being deployed**
  - CONUS Complete, EUR/PAC installs in progress
- **LSC APL Status**
  - REDCOM added to APL
  - Nokia Simens Networks has stopped marketing and selling their product. DISA is awaiting formal notification on the future of their product line
- **Commercial Cost Avoidance Feature**
  - Avaya, REDCOM ready today
  - Cisco has testing planned May/June 2012

APL Definition Per 8100.04 and Process

The UC APL is the single authoritative source for certified UC products intended for use on DoD networks.



UC APL Categories



CJCSI 6212.01E and the UC APL

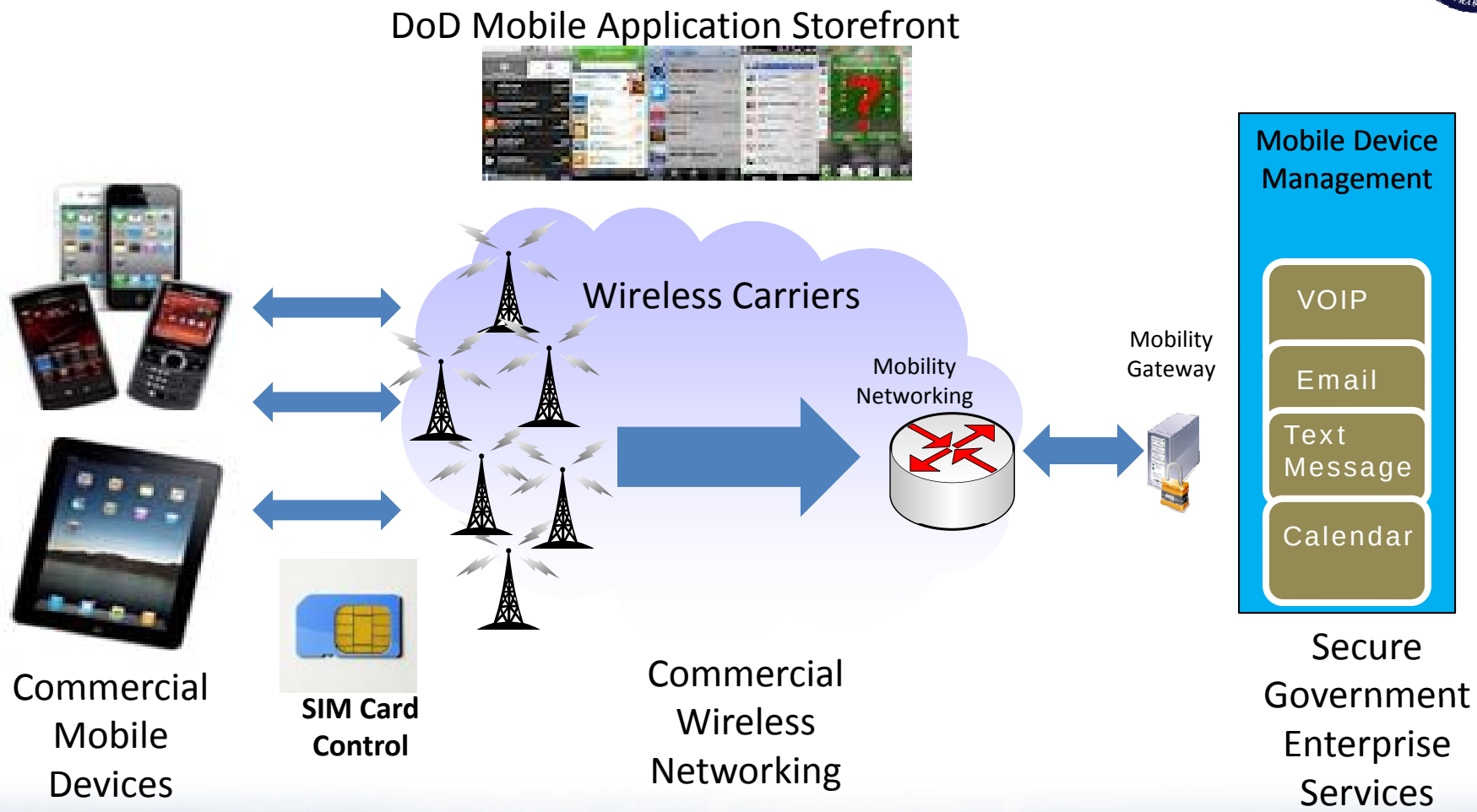
	6212.01E	UCR APL
Requirements	NR-KPP from, for example, Information Support Plan (ISP) or Tailored Information Support Plan (TISP)	UCR 2008
Scope	All Information Technology (IT) and National Security Systems (NSS)	Equipment and software, whether systems or services, which provide or support UC voice, video or data services
Environment	Specific implementation, tested in an operationally realistic environment	Basic configuration, tested against baseline IO and IA requirements.
Certification	NR-KPP based interoperability certification of system	Special Interoperability Certification of IO and IA requirements in the UCR 2008. Placement of product on UC APL.

Mutually supporting

UC APL products can be used as building blocks on major programs reducing test times

UCR requirements can support the development of ISPs and TISPs for major programs

Mobility End-to-End Strategy



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

Unclassified Capability Delivery

	Phase 1 (Unclass Focused)			Phase 2 (Convergence)
	May-June 2012	July-Oct 2012	Nov 2012- Mar 2013	Apr-Aug 2013
Mobile Capability - Spiral Test Strategy & Deployment				
Phases	**Spiral 1**	**Spiral 2**	**Spiral 3**	**Multiple**
Unclassified Units Deployed Goals	50 (Android) / 50 (iOS)	300 (150 Android / 150 iOS)/Playbooks	1500 (Android / iOS mix)	6500 (Android / iOS mix)
User Capability Deployed	STIG'd Smart Phone	STIG'd Smart Phone	STIG'd Smart Phone	STIG'd Smart Phone with Smart Phone APL
	Carrier Access	Carrier Access with Device Validator and VPN	Multiple Carrier Access with PKI enabled VPN	Multiple Carrier Access with Worldwide Service with PKI enabled VPN
	Pre-loaded Apps	Pre-loaded Apps	10-12 Enterprise Apps on Initial App Store	Certified Apps on App Storefront (tiered Stores)
	Enterprise Email	Enterprise Email	Enterprise Email + Service Interface	Enterprise Email Depart Unique Email
		VoIP Calling to DISN	VoIP Calling to DISN	VoIP Calling to DISN
	Initial MDM Capability (Via Good)	Initial MDM Capability (Via Good) MDM/MAS Solicitation	Initial Enterprise MDM, BackOffice and MAS	Objective Enterprise MDM, BackOffice and MAS

Begin Offering as Subscription Based Service in FY 14

DISA Mobility T&E

Must ensure enterprise solutions are tested to the mobility edge

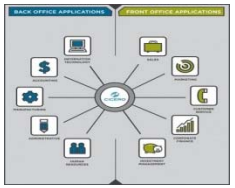
Network operations and Helpdesk

Operations Support Systems

Unclassified* - Mobility Network Infrastructure - *Classified

Common Services

Mobile App Storefront



Mobile Device Mgmt

Commercial Carrier

Devices & Platforms

Business Support Systems

Experience must be consistent across devices

Apps must be secure and interoperate

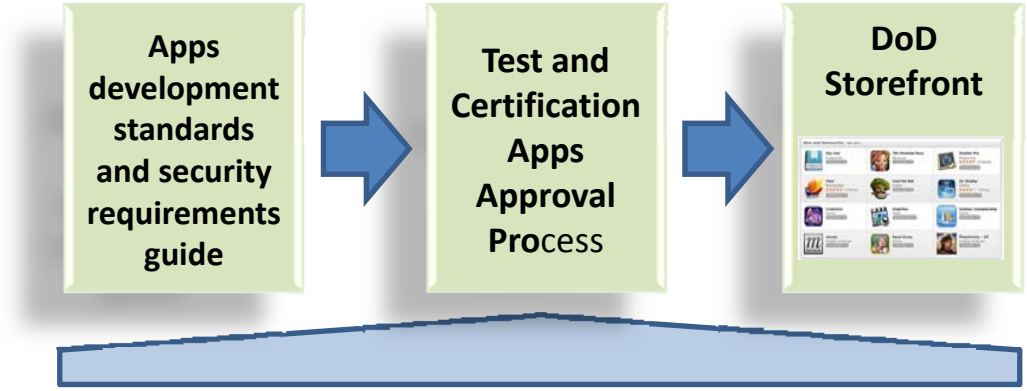
Device mgmt must meets DoD policy requirements

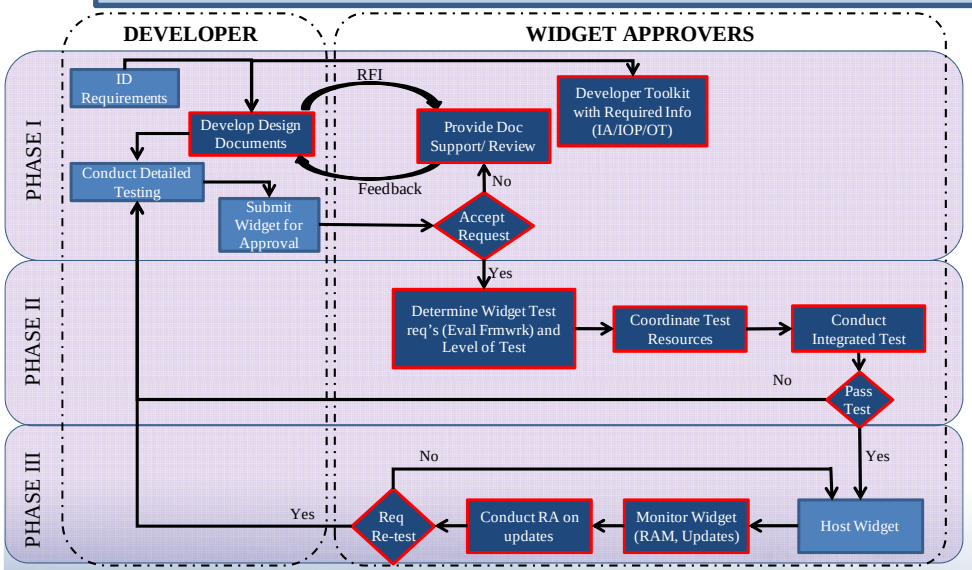
Carriers must connect and perform IAW DISA standards

Devices must meet UC/APL requirements

Tested DoD Mobility infrastructure using certified mobile applications, devices, components, and services providing DoD secure, reliable, and interoperable capabilities

DoD Mobility Test & Certification Evolving Apps Approval Process

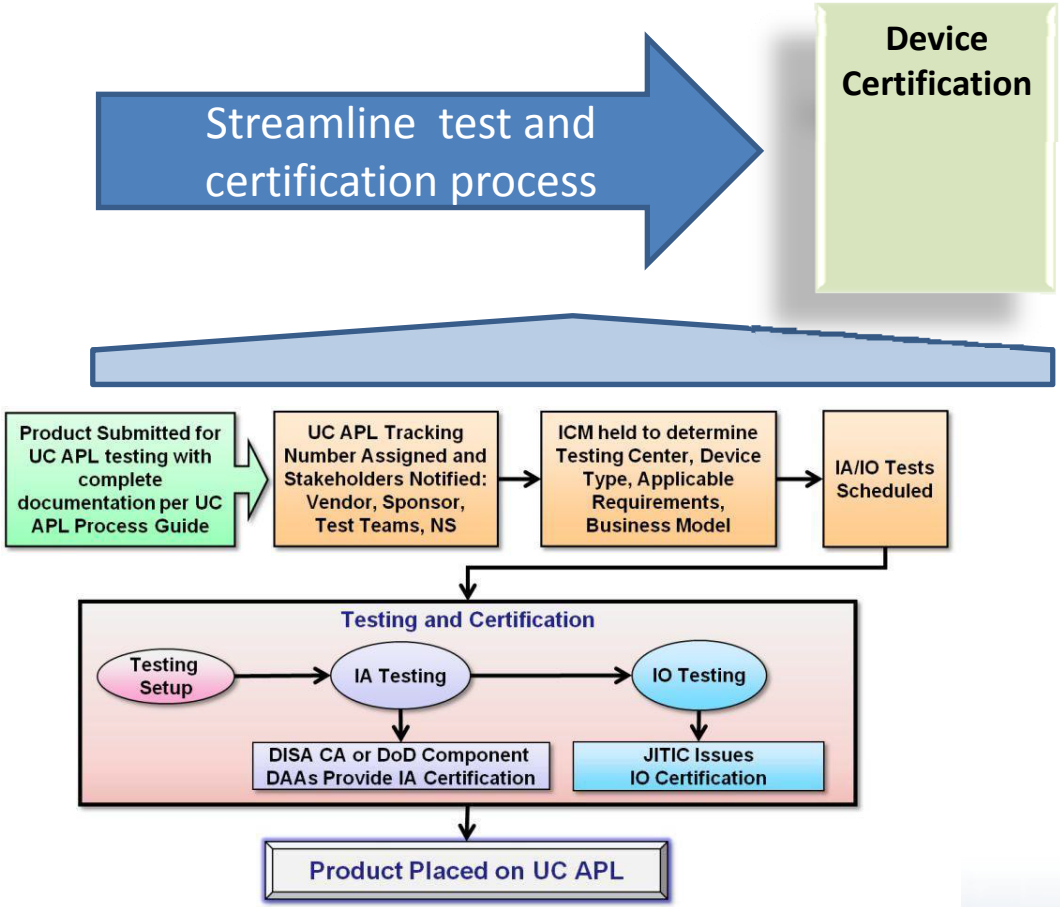




- Establish software standards for developers and vendors via published security requirements guide
- Develop an accelerated approval process for new mobile apps
- Test and certify adherence to published standards and guidance prior to provisioning apps to DoD storefront.

Providing mobile apps developers sand vendors standards and guidance are key to accelerating the provisioning of capabilities to the DoD Storefront

DoD Mobility T&E Evolving Device/Platform Approval Process



- DISA will release security requirements guides (SRGs) to provide developers with the agency's security requirements for devices and the modifications necessary to meet government needs.

- Accelerate security review process to avoid smartphones being obsolete by the time they're allowed to connect to Defense networks.

- Evolve faster ways to test and certify mobile devices/platforms

Maintain test rigor while dramatically accelerating the certification of mobile devices

	Phase 1			Phase 2	Phase 3
	Spiral 1 (Months 1-2)	**Spiral 2 (Months 2-5)**	**Spiral 3 (Months 5-9)**	**(Months 9- 15)**	**(Months 15+)**
Event Scope	50 Android/50 iOS 1 Carrier	150 Android/150 iOS 2 Carrier	1500 SBU mix Multiple Carriers	5000 SBU 1500 Classified Multiple Carriers	Operational Multiple Carriers
Capabilities					Operational Effective, Suitable. Interoperable, and Secure (OESIS) determination
Mobile Device	User Experience Assess Caps /Lims	User Experience Assess Caps /Lims	User Experience Assess Caps/Lims Performance(1)	User Experience Assess Caps/Lims Performance (1)	
Mobile Device Management (MDM)	Observations/ Lessons Learned	User Experience Assess Caps/Lims	User Experience Assess Caps/Lims Performance (4)	User Experience Assess Caps/Lims Performance (4)	
Mobile Apps Store (MAS)	N/A	N/A	User Experience Assess Cap/Lims	User Experience Assess Cap/Lims Performance	
Operational Support Systems (OSS)	N/A	User Experience Assess Cap/Lims	User Experience Assess Cap/Lims Performance	User Experience Assess Cap/Lims Performance	
Business Support Systems (BSS)	N/A	User Experience Assess Cap/Lims	User Experience Assess Cap/Lims Performance	User Experience Assess Cap/Lims Performance	
DoD Mobile Network	Observations/ Lessons Learned	Assess Caps/Lims	User Experience Assess Caps/Lims Performance (3)	User Experience Assess Caps/Lims Performance(3)	
Carrier Network	Observations/ Lessons Learned	Assess Caps/Lims	User Experience Assess Caps/Lims Performance (2)	User Experience Assess Caps/Lims Performance(2)	
Enterprise Services					
Enterprise Email	User Experience Assess Caps /Lims	User Experience Assess Caps /Lims	User Experience Assess Caps /Lims	User Experience Assess Caps/Lims	
Mobile Apps	Pre-loaded User Experience Assess Caps/Lims	Pre-loaded User Experience Assess Caps/Lims [Enterprise Services]	via MAS User Experience Assess Caps/Lims	via MAS User Experience Assess Caps/Lims	
Calendar	User Experience Assess Caps/Lims	User Experience Assess Caps/Lims	User Experience Assess Caps/Lims	User Experience Assess Caps/Lims	
VOIP	N/A	User Experience Assess Caps/Lims	User Experience Assess Caps/Lims	User Experience Assess Caps/Lims	
Support Services					
Training	Observations/ Lessons Learned	User Experience Assess Caps/Lims	User Experience Assess Caps/Lims	User Experience Assess Caps/Lims	
Helpdesk	Observations/ Lessons Learned	User Experience Assess Caps/Lims	User Experience Assess Caps/Lims Performance (2)	User Experience Assess Caps/Lims Performance(2)	

DISA
A Combat Support Agency