Department of Defense (DoD)
Unified Capabilities Master Plan (UC MP)

October 2011

DoD Chief Information Officer

Department of Defense (DoD)
Unified Capabilities Master Plan (UC MP)

The purpose of the "Department of Defense (DoD) Unified Capabilities (UC) Master Plan (UC MP)" is to define the implementation strategy to converged, net-centric, IP-based enterprise UC as required by DoD Instruction (DoDI) 8100.04, "DoD Unified Capabilities." The UC MP serves as a guideline to the DoD Components in the preparation of implementation and acquisition plans for phasing in voice and video over IP services, and other UC that shall operate in converged voice, video, and/or data networks. The UC MP addresses synchronization of life-cycle activities, from acquisition to operations to sustainment until retirement, for DoD networks that provide UC. The UC MP provides guidance for DoD Component Program Objective Memorandum submissions.

Approved by: ______________________

Teresa M. Takai
Department of Defense
Chief Information Officer

Date: 3 Oct 2011

Executive Summary

ES.1. PURPOSE. The purpose of the "Department of Defense (DoD) Unified Capabilities (UC) Master Plan (UC MP)," as directed by DoD Instruction (DoDI) 8100.04, "DoD Unified Capabilities," is to define the implementation strategy for converged, Internet Protocol (IP)-based enterprise UC; serve as a guideline to the DoD Components in the preparation of implementation and acquisition plans for phasing in voice, video, and data over IP services provided on converged networks that support UC; and provide guidance for DoD Component Program Objective Memorandum (POM) submissions. UC is defined as the integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness for DoD Components.

ES.2. APPLICABILITY. Per DoDI 8100.04, the UC MP applies to DoD Component planning, investment, development, acquisition, operations, and management of DoD networks to support UC, independent of the mix of technologies (e.g., circuit-switched and/or IP), and whether converged or non-converged, including all equipment or software (hereafter referred to as "UC products" or "products") and services that provide or support UC, throughout a product's life-cycle activities, from acquisition to operations to sustainment until retirement, for DoD networks that provide UC. The UC MP is applicable to acquisition of services as described in DoD Directive 5000.01 and DoD Instruction 5000.02, however, is not applicable to other DoD Component acquisition programs governed by these DoD issuances. DoD Components are encouraged to use UC-certified products in developing acquisition programs, where appropriate.

ES.3. UNIFIED CAPABILITIES OPERATIONAL FRAMEWORK. This framework is intended to guide and align DoD Component instantiation of respective implementation plans and solutions. It provides a common language and reference for DoD Components' implementation of UC technology, supports implementation of DoD Component solutions, and encourages adherence to common standards and specifications. All DoD Components shall develop and align respective Component implementation plans within this framework, consistent with the constraints of DoD Component resources, mission needs, and business cases. The transition will begin starting in Fiscal Year (FY) 2012. DoD Components implementation plans shall support individual mission requirements, business cases, and most cost effective implementation of enterprise UC. Per Reference (a), all networks that support UC shall use certified products on the DoD UC Approved Products List (APL), which may be found at http://disa.mil/ucco. Beginning in FY 14, DoD Components shall be responsible for ensuring compliance with this operational framework.

a. The UC Operational Framework enables strategic, tactical, classified, and multinational missions with a broad range of interoperable and secure capabilities for converged non-assured and assured voice, video, and data services from the end device, through Local Area Networks (LANs), and across the backbone networks.

b. This operational framework is based on the extensive work already accomplished by DISA through laboratory and pilot testing using interoperable and secure products from the DoD UC APL, and deploying those products in the Defense Information Systems Network (DISN) backbone infrastructure. As a result of the progress made to date, DoD has already begun deployment of approved IP-based products. This operational framework leverages IP technologies, and DoD aggregated buying power, to provide enterprise UC solutions by collaboration between DISA, as the backbone and edge services provider, and the other DoD Components, as the edge services and infrastructure providers and users.

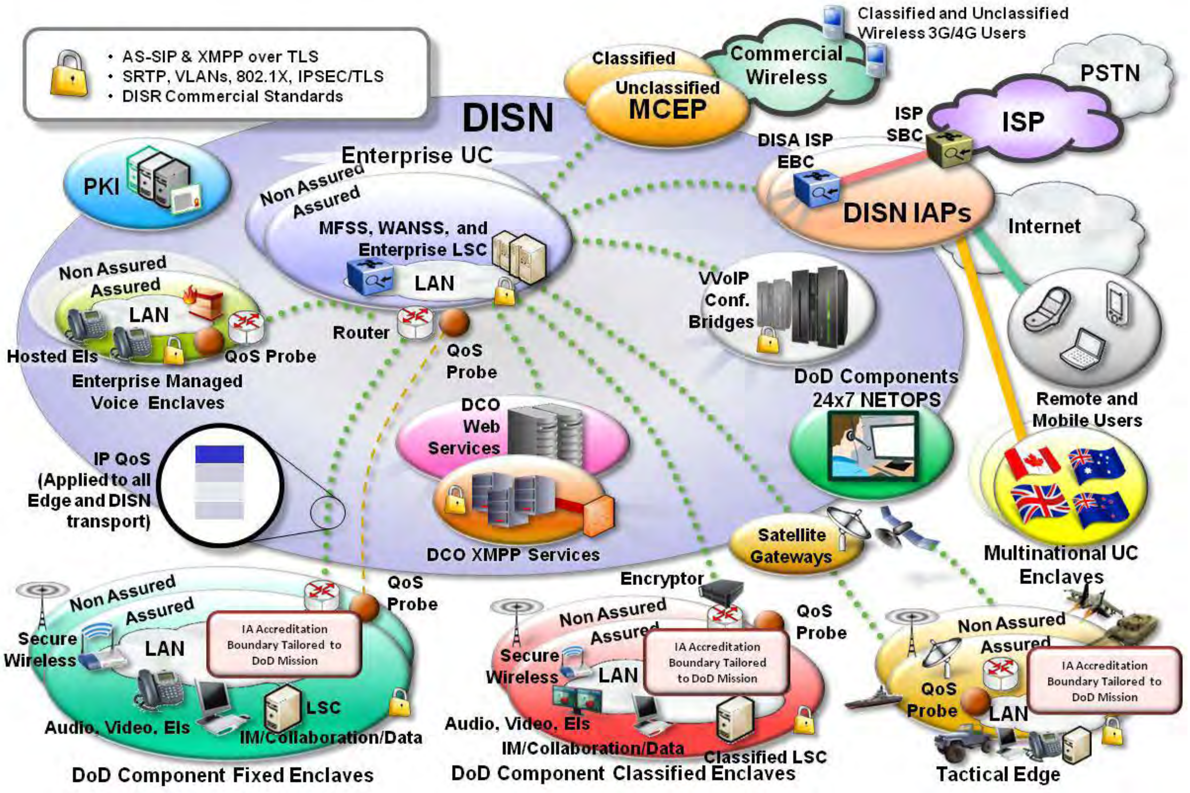

Figure ES.1. UC High Level Operational Framework

c. This operational framework is consistent with Secretary of Defense Memorandum, "Department of Defense (DoD) Efficiency Initiatives," August 16, 2010, and corresponding enterprise UC initiatives. By implementing enterprise multi-vendor UC investment in, and operating costs for, those services may be reduced using common and standard service models.

d. This operational framework leverages the requirements of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)) Publication, “Department of Defense Unified Capabilities Requirements (UCR),” which has been coordinated with DoD Components and industry.

ES.4. UC IMPLEMENTATION STRATEGY. The UC implementation strategy supports the Secretary of Defense efficiency initiatives for unclassified and classified enterprise UC. UC implementation is based on the following precepts:

a. Drive technology insertion through a common UC operational framework.

b. Transition to UC using implementation phases defined by each DoD Component, as specified in respective DoD Component implementation plans. DISA and the other DoD Components shall collaboratively integrate these implementation phases to maintain consistency and integrity of the UC operational framework and to manage overall DoD UC risks.

c. Employ prototype, preproduction, multi-vendor, and UC Pilot test and evaluation activities to ensure products are interoperable, secure, and NetOps compliant.

d. Use competitive multi-vendor approved products based on common user requirements and listed on the DoD UC APL.

e. Ensure Quality of Service (QoS) is available end-to-end, independent of technology employed, for non-assured/assured UC.

f. Reduce Defense Red Switch Network (DRSN) footprint by revalidating user requirements, migrating users, as appropriate, to classified DISN voice services such as Voice over Secure IP (VoSIP), investing in an IP-capable DRSN, and enabling gateways among DoD classified voice networks.

g. Provide UC across DoD and commercial networks using commercial standards, as appropriate.

h. Implement end-to-end UC at a pace consistent with respective DoD Component mission requirements and available resources. DoD Components shall coordinate with DISA on UC implementation schedules to ensure synchronization across the DoD enterprise.

i. Use the DoD identity management and access control process.

ES.5. Organizational Relationships/Responsibilities. Figure ES.2 defines the organization relationships among the UC key stakeholders consisting of the DoD CIO, Joint Staff, DISA, and the DoD Components over the life cycle of UC, from acquisition to operations to sustainment until retirement. The DoD CIO is responsible for UC policy, requirements, and overarching planning documents. The notional governance structure for UC is established in DoDI 8100.04. Final governance structure for UC implementation shall be determined when Secretary of Defense reorganization efficiencies initiatives are complete. The Joint Staff is responsible for developing and issuing UC implementing instructions. DISA is responsible for UC enterprise funding, engineering, acquisitions, operations, maintenance, and sustainment associated with the DISN backbone. Additionally, DISA shall provide a Blanket Purchase Agreement (BPA) for the other DoD Components to use to acquire edge infrastructure UC APL products. The use of the

DISA BPA is recommended by all DoD Components. DoD Components are responsible for edge infrastructure funding, engineering, acquisitions, and operations.

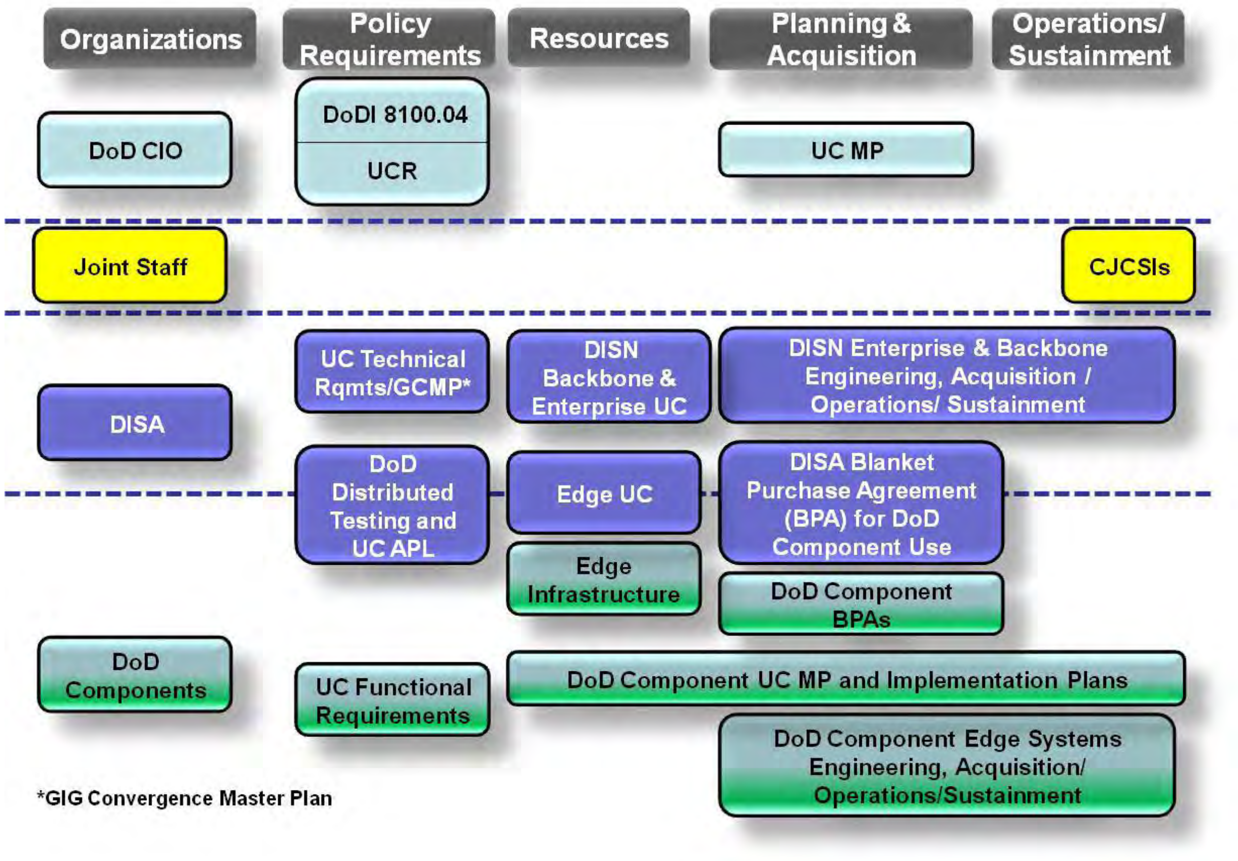
Organizations
Policy Requirements
Resources
Planning & Acquisition
Operations/ Sustainment
DoD CIO
DoDI 8100.04
UCR
UC MP
Joint Staff
CJCSIs
DISA
UC Technical Rqmts/GCMP*
DISN Backbone & Enterprise UC
DISN Enterprise & Backbone Engineering, Acquisition / Operations/ Sustainment
DoD Distributed Testing and UC APL
Edge UC
DISA Blanket Purchase Agreement (BPA) for DoD Component Use
Edge Infrastructure
DoD Component BPAs
DoD Components
UC Functional Requirements
DoD Component UC MP and Implementation Plans
DoD Component Edge Systems Engineering, Acquisition/ Operations/Sustainment
*GIG Convergence Master Plan

Figure ES.2. Organizational Relationships/Responsibilities

ES.6. RESOURCE PLANNING AND RESPONSIBILITIES. To focus limited DoD Component resources, existing circuit switch technologies shall be replaced with more capable, cost effective, and sustainable enterprise UC APL products compliant with the UC operational framework and UCR. For the period FY 12-16, existing network infrastructure modernization and technology refresh funding shall be used to implement enterprise UC by all DoD Components. DISA and the other DoD Components shall execute the following resource responsibilities:

a. DISA shall:

(1) In collaboration with the other DoD Components, lead the development of an initial Business Case Analysis (BCA) to meet the end-to-end requirements of the UC operational framework within 180 days of issuance of the UC MP for the DoD CIO Executive Board's assessment, and the Department's decision-making processes. The Director, Cost Assessment and Program Evaluation (CAPE) shall review and approve this BCA. The BCA must aggregate the implementation of UC on DISN backbone, DISN common and edge UC, and incorporate each DoD Component's BCA for UC implementation.

(2) Develop, in collaboration with the other DoD Components, an end-to-end DoD Enterprise UC Implementation Plan within 120 days of issuance of the UC MP.

(3) Based on the CAPE-approved BCA, fund unclassified and classified enterprise UC per the priority identified in the DISA UC Implementation Plan.

(4) Establish a BPA, within 180 days of issuance of the UC MP, for use by all DoD Components to acquire, at volume discounts, the UC APL products needed for edge UC infrastructure implementation.

b. DoD Components shall:

(1) In collaboration with DISA, support and provide input in the development of a BCA to meet the end-to-end requirements of the UC operational framework.

(2) Develop, in collaboration with DISA, the respective DoD Component UC Implementation Plans within 120 days of issuance of the UC MP.

(3) Based on the CAPE-approved BCA, prioritize existing FY 12/13 UC network infrastructure modernization and technology refreshment investments and operations and maintenance budgets to implement UC, consistent with respective DoD Component's missions and resources.

(4) Based on the CAPE-approved BCA, identify FY 14 POM investments, operations, and sustainment funding needed to implement UC within respective DoD Components' implementation plans.

<u>TABLE OF CONTENTS</u>

TABLES

FIGURES

1. PURPOSE. The purpose of the "Department of Defense (DoD) Unified Capabilities (UC) Master Plan (UC MP)" (hereafter referred to as "UC MP"), as directed by DoD Instruction (DoDI) 8100.04, "DoD Unified Capabilities" (Reference (a)), is:

a. To define the implementation strategy for converged, Internet Protocol (IP)-based enterprise UC.

b. To serve as a guideline to the DoD Components in the preparation of implementation and acquisition plans for phasing in voice, video, and data over IP services provided on converged networks that support UC.

c. To provide guidance for DoD Component Program Objective Memorandum (POM) submissions.

2. APPLICABILITY. Per Reference (a), the UC MP applies to:

a. The Office of the Secretary of Defense (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").

b. DoD Component planning, investment, development, acquisition, operations, and management of DoD networks to support UC, independent of the mix of technologies (e.g., circuit-switched and/or IP), and whether converged or non-converged, including all equipment or software (hereafter referred to as "UC products" or "products") and services that provide or support UC, throughout a product's life-cycle activities, from acquisition to operations to sustainment until retirement, for DoD networks that provide UC.

c. Acquisition of services as described in DoD Directive (DoDD) 5000.01 (Reference (b)) and DoDI 5000.02 (Reference (c)).

d. This UC MP does not apply to DoD Component acquisition programs governed by References (b) and (c) except as stated above, however, the DoD Components are encouraged to use UC-certified products in developing acquisition programs, where appropriate.

3. POLICY, REQUIREMENTS, AND PLANNING DOCUMENTATION FOR UC IMPLEMENTATION. This section provides a broad overview of requirements for DoD Component planning, investment, development, acquisition, operations, sustainment, and management of DoD networks that provide UC.

a. UC provides the integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness for DoD Components. UC integrates standards-based communication and collaboration services including, but not limited to, messaging; voice, video, and web conferencing; and unified communication and collaboration applications or clients. These standards-based services shall be integrated with available enterprise UC within business, intelligence, and warfighting communities. Capabilities are provided to DoD fixed, mobile, and tactical users as well as authorized U.S. Government interagency and multinational mission partners, and includes ground, air, space and seaborne platforms, as appropriate.

b. The UC requirements process addresses DoD-level strategic, operational, tactical, and intelligence community needs based on approved DoD architectures and Joint Staff validated requirements, to include those documented in the Global Information Grid (GIG) 2.0 ICD and annual Capability Gap Assessments. These UC requirements shall be reflected in Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) Publication, "Department of Defense Unified Capabilities Requirements (UCR)" (Reference (d)), this UC MP, and subsequent DoD Component UC implementation plans.

c. Per Reference (a), DoDI 8100.04, implementation of UC across DoD is dependent on UC transport, which is the secure and highly available enterprise network infrastructure used to provide voice, video, and/or data services through a combination of DoD and commercial terrestrial, wireless, and satellite communications (SATCOM) capabilities.

d. Implementation of UC is required to meet the requirements of the IP-enabled battlefield of the future. UC allows the DoD to achieve the following strategic, tactical, and intelligence community needs:

(1) Ubiquitous, robust, and scalable DoD networks, enabling integrated operations.

(2) IP-addressed sensors, munitions, biosensors, and logistics tracking applications, which shall enhance situational assessments and information availability.

(3) End device-to-end device security, authentication, and non-repudiation, which shall enable new information assurance strategies that support mission assurance.

(4) Increased operations tempo supported by rapid reorganizational capabilities, shared situational awareness, and improved wireless and mobility support.

(5) Greater support for mobility and communications on the move.

(6) Dynamic formation of a Community of Interest (COI) supported by improved multicasting.

(7) Real-time collaboration using integrated voice, video, and data capabilities.

(8) Situational awareness using Network Operations (NetOps) COI information sharing.

(9) Rapid and agile information technology infrastructures with the capability to "discover" adjacent networks and plug and play to facilitate quicker, more dynamic responses.

e. Figure 1 depicts the policy, requirements, and planning documentation for UC implementation.

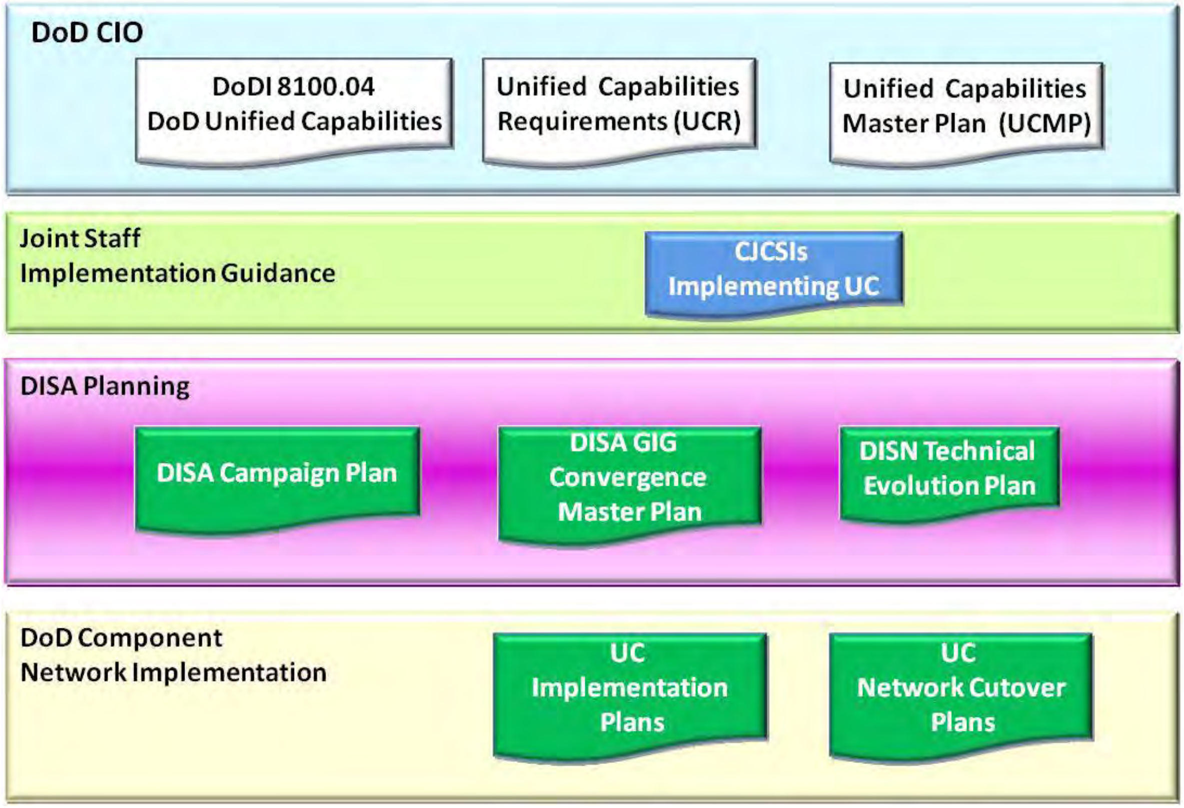
DoD CIO
DoDI 8100.04 DoD Unified Capabilities
Unified Capabilities Requirements (UCR)
Unified Capabilities Master Plan (UCMP)
Joint Staff Implementation Guidance
CJCSIs Implementing UC
DISA Planning
DISA Campaign Plan
DISA GIG Convergence Master Plan
DISN Technical Evolution Plan
DoD Component Network Implementation
UC Implementation Plans
UC Network Cutover Plans

Figure 1. Policy, Requirements, and Planning Documentation

(1) The four key DoD Chief Information Officer (DoD CIO) documents that drive UC implementation are:

(a) Secretary of Defense Memorandum, "Department of Defense (DoD) Efficiency Initiatives" (Reference (e)), which directs the Department to "consolidate DoD's IT infrastructure where possible, to achieve greater economies of scale." The goals of Reference (e) are "to reduce duplication, overhead, and excess, and instill a culture of savings and restraint across the DoD." The Department shall achieve these goals and deliver a streamlined, rationalized, and simpler network by consolidating IT infrastructure across DoD. The UC MP addresses the enterprise UC supporting Reference (e).

(b) Reference (a), which 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. Additionally, it establishes the governing policy for UC products and services supported on DoD networks.

(c) Reference (d), which specifies the functional requirements, performance objectives, and technical specifications for DoD networks that support UC, and supports test, certification, acquisition, connection, and operation of these devices.

(d) The UC MP, which defines the UC operational framework and strategy for converged, net-centric, IP-based enterprise UC. It serves as a guideline to the DoD Components in the preparation of implementation plans and acquisition plans for phasing in enterprise UC. It initially focuses on unified capabilities that can be matured and fielded by FY 16 within the constraints of DoD Component resources, mission needs, and business cases. The UC MP will be updated biennially, as required.

(2) The Joint Staff publishes, as appropriate, implementing instructions for UC based on DoD CIO's direction and guidance.

(3) The major Defense Information Systems Agency (DISA) planning documents driving and supporting UC activities are:

(a) The "DISA Campaign Plan," identifies three Lines of Operations: Enterprise Infrastructure; Command and Control (C2) and Information Sharing; and Operate and Assure, with specific tasks for UC implementation.

(b) The "DISA GIG Convergence Master Plan," identifies five categories of DISA programs: Application, Services, and Data; Communications and Networks; Information Assurance; Network Operations and Enterprise Management; and Computing Infrastructure.

(c) The "Defense Information Systems Network (DISN) Technical Evolution Plan (DTEP)," based on the DISN Overarching Technical Strategy (DOTS), addresses the plan for DISN UC technical implementation. The DTEP describes the plan for DISN technical refresh funds to augment and sustain the DISN. The DTEP also addresses technology implementation requirements outlined in Reference (d). The DTEP's four capability areas are: Information Assurance, Connectivity, Network Management, and Interoperability.

(4) Documents essential to synchronizing investments across DoD, by DoD Components, are:

(a) The DoD Component UC implementation plans shall synchronize the specific deployments of UC from a converged, consolidated, and integrated family of commercial and DoD networks perspective, based on DoD Components' acquisition plans. DoD Component UC implementation plans shall be used to address detailed costs, funding, schedules and transition phases, and system designs to be implemented. DoD Component UC implementation plans shall be based on the proven risk management process used for UC which includes the development of UC requirements based on collaboration with DoD Components and industry, DoD CIO sponsored and DISA hosted multi-vendor test events at DoD Component test laboratories, UC Spirals for operational validation based on DISN UC CONOPS (Reference (f)), resulting in DoD UC approved products.

(b) DoD Component UC Network Cutover Plans (NCPs) shall ensure site and transport readiness, security of mobile devices, and integration with DoD and commercial networks. DoD Components' UC NCPs shall be used to facilitate the DISN connection approval process to fulfill DoD Component UC service requests.

4. UNIFIED CAPABILITIES OPERATIONAL FRAMEWORK. This framework is intended to guide and align DoD Component instantiation of respective implementation plans and solutions. It provides a common language and reference for DoD Components' implementation of UC technology, supports implementation of DoD Component solutions, and encourages adherence to common standards and specifications. All DoD Components shall develop and align respective Component implementation plans within this framework, consistent with the constraints of DoD Component resources, mission needs, and business cases. The transition will begin starting in FY 12. DoD Components implementation plans shall support individual mission requirements, business cases, and most cost effective implementation of enterprise UC. Per Reference (a), all networks that support UC shall use certified products on the DoD UC Approved Products List (APL), which may be found at http://disa.mil/ucco. Beginning in FY 14, DoD Components shall be responsible for ensuring compliance with this operational framework.

a. Overview and Summary

(1) The UC High Level Operational Framework, illustrated in Figure 2, enables strategic, tactical, classified, and multinational missions with a broad range of interoperable and secure capabilities for converged non-assured and assured voice, video, and data services from the end device, through Local Area Networks (LANs), and across the backbone networks.

(2) This operational framework is based on the extensive work already accomplished by DISA through laboratory and pilot testing using interoperable and secure products from the DoD UC APL, and deploying those products in the Defense Information Systems Network (DISN) backbone infrastructure. As a result of the progress made to date, DoD has already begun deployment of approved IP-based products. This operational framework leverages IP technologies, and DoD aggregated buying power, to provide enterprise UC solutions by collaboration between DISA, as the backbone and edge services provider, and the other DoD Components, as the edge services and infrastructure providers and users.

(3) This operational framework is consistent with Reference (e) goals and corresponding enterprise UC initiatives. By implementing enterprise multi-vendor UC investment in, and operating costs for, those services may be reduced using common and standard service models. Implementation of enterprise UC can provide a full range of related capabilities to all DoD users from central locations that leverage the DISN, and IP technologies. This approach minimizes potential duplication of costs that may occur for UC operations and maintenance, network operations, sustainment, and information assurance at DoD Component locations worldwide.

(4) This operational framework leverages the requirements of the UCR (Reference (d)), which has been coordinated with DoD Components and industry.

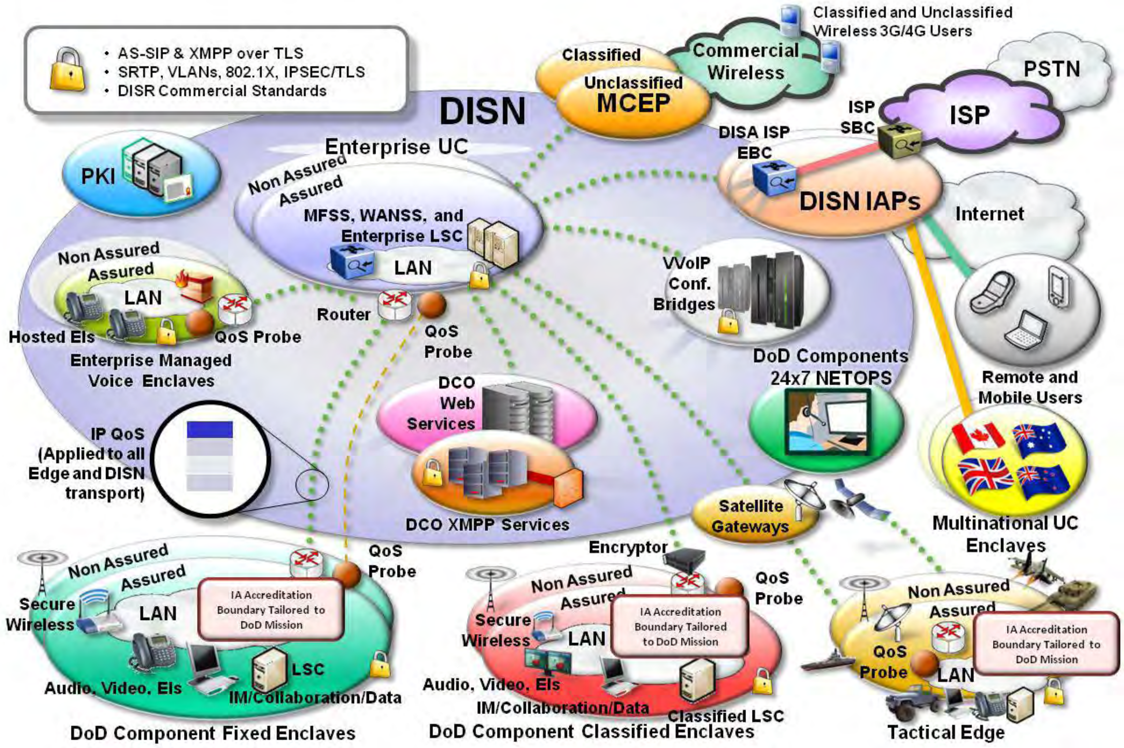

Figure 2. UC High Level Operational Framework

(5) This operational framework shall continue to evolve as it is tested via multi-vendor tests events, demonstrated via conduct of enterprise product solutions at DoD test laboratories, and implemented using planned UC pilot test and evaluation activities. The UCR (Reference (d)) shall be updated based on multi-vendor test events independently evaluated results.

b. Enterprise UC Vision. Figure 3 describes the vision for unclassified and classified enterprise UC, enterprise and edge infrastructures, and secure access to various other networks:

(1) The unclassified and classified enterprise UC, in priority order for implementation during the period of FY 12 to FY 16, include:

(a) Non-Assured/Assured Voice, Video, and Data Session Management: provides enterprise point-to-point UC, independent of the technology (circuit switched or IP). Per Reference (d), capabilities include, but are not limited to, end device registration, session establishment and termination, and UC session features (e.g., Assured Services Admission Control, Call Hold, Call Transfer, etc.).

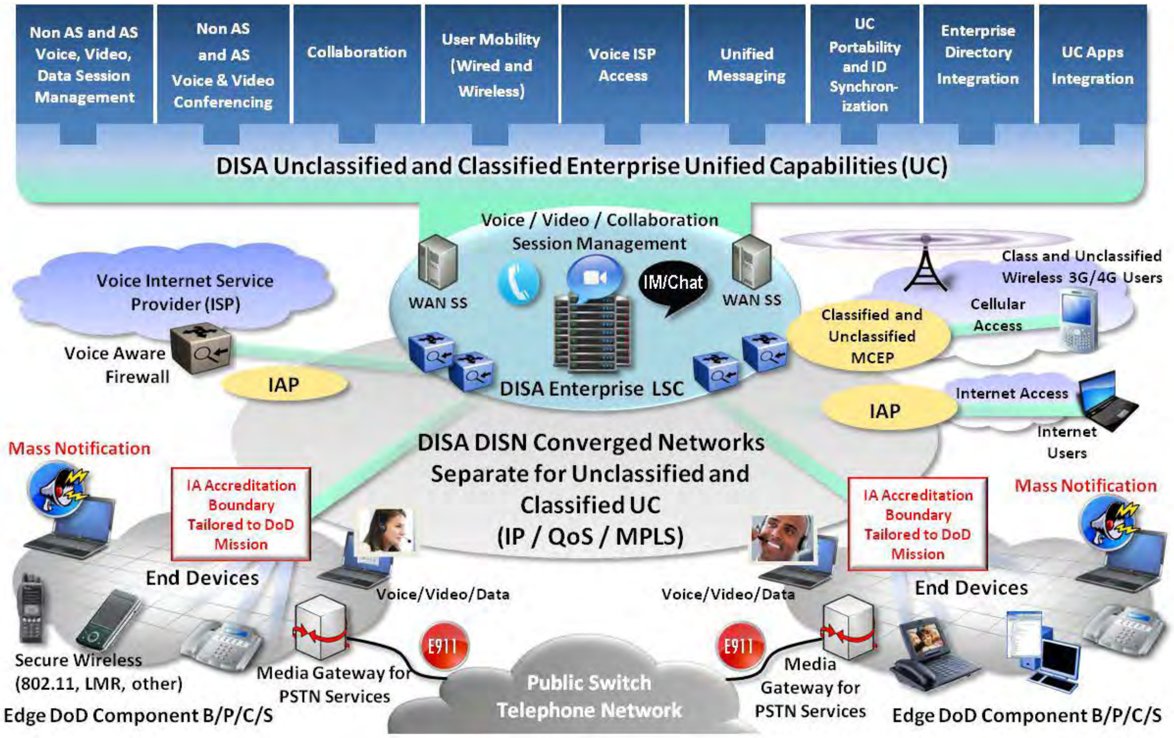
Non AS and AS Voice, Video, Data Session Management
Non AS and AS Voice & Video Conferencing
Collaboration
User Mobility (Wired and Wireless)
Voice ISP Access
Unified Messaging
UC Portability and ID Synchronization
Enterprise Directory Integration
UC Apps Integration
DISA Unclassified and Classified Enterprise Unified Capabilities (UC)
Voice / Video / Collaboration Session Management
WAN SS
IM/Chat
WAN SS
Voice Internet Service Provider (ISP)
Voice Aware Firewall
IAP
DISA Enterprise LSC
Classified and Unclassified MCEP
Class and Unclassified Wireless 3G/4G Users
Cellular Access
IAP
Internet Access
Internet Users
Mass Notification
IA Accreditation Boundary Tailored to DoD Mission
DISA DISN Converged Networks Separate for Unclassified and Classified UC (IP / QoS / MPLS)
IA Accreditation Boundary Tailored to DoD Mission
Mass Notification
End Devices
Voice/Video/Data
Voice/Video/Data
End Devices
Secure Wireless (802.11, LMR, other)
Media Gateway for PSTN Services
E911
Public Switch Telephone Network
E911
Media Gateway for PSTN Services
Edge DoD Component B/P/C/S
Edge DoD Component B/P/C/S

Figure 3. Enterprise UC Vision

(b) Non-Assured/Assured Voice and Video Conferencing: provides the ability to conference multiple voice or video subscribers with a variety of room controls for displays of the participants. It also includes an optional component that allows subscribers to schedule conferences.

(c) Collaboration: provides IP-based solutions that allow subscribers to collaborate (e.g., instant messaging, chat, presence, and web conferencing).

(d) User Mobility (wired and wireless): provides the ability to offer wireless and wired access, for UC supported by multifunction mobile devices. In addition, it provides access to enterprise UC globally using UC portability.

(e) Voice Internet Service Provider (ISP) Access: provides unclassified and classified enterprise UC for access to commercial voice services over IP. This service provides both local and long distance dialing capability using commercial ISPs via secure interconnections.

(f) Unified Messaging: provides the integration of voicemail and e-mail. The integration of these two capabilities allows subscribers to access voicemail via e-mail or access e-mail via voicemail.

(g) UC Portability and Identity Synchronization: provides an enterprise UC systematic approach to portability functions (e.g., repository of user profiles and privileges, and subscriber identification and authentication). Uses DISA's existing ID Synchronization service as the primary service for DoD ID Synchronization.

(h) Enterprise Directory Integration: integrates UC with repository of subscriber contact information accessible to all authorized and authenticated subscribers.

(i) UC Applications Integration: supports mission and business applications integration with the enterprise UC (e.g., integration of UC provided presence with DoD Component-owned business applications).

(2) The Enterprise Local Session Controller (ELSC) centrally provides the functionality essential for delivering enterprise non-assured and assured services securely across a quality of service enabled network using multiple vendor products. When IP access to the ISP is implemented, all connections shall be managed by the ELSC to centrally protect the network. Requirements for the ELSC (derived from current LSC specifications) shall be specified in Reference (d), beginning with UCR 2008, Change 3 and issued by September 30, 2011. ELSCs may be deployed by individual DoD Components during the transition period to the UC operational framework.

(3) The DoD Component edge infrastructure provides non-assured and assured enterprise services to the end user fixed or mobile devices. The edge infrastructures can consist of either a separate security enclave, or regional enclaves connected to the DISN core infrastructure. The edge includes non-assured and/or assured LANs (wired and wireless) tailored to meet mission needs that support converged UC consistent with DoD Component implementation plans. Consistent with DoD Component mission requirements and resources constraints, access to the Public Switched Telephone Network (PSTN) shall be via circuit switches until secure access to the ISP is accomplished centrally at the DISA Internet Access Point and ELSC, at which time the DoD Component may decide to migrate to an ISP offering, as appropriate. The UC operational framework shall support local Enhanced 911 (E911), mass notification services, and critical emergency response capabilities. User requirements for non-assured and assured services shall be determined by the appropriate DoD Component.

c. High Level Operational Concept

(1) DISN Backbone Infrastructure. Figure 4 illustrates the DISN backbone infrastructure for up to 22 locations globally supporting a set of Geographic Regions (GeoRegions) based on DoD populations in CONUS and OCONUS as part of the DISN investments and the DISN Subscription Services (DSS). This backbone shall make available services to user end devices for DoD Component locations depending on individual DoD Component’s mission requirements. Final decisions on the GeoRegions shall be made as part of the DoD Components' collaborative UC Implementation Plan integration activities.

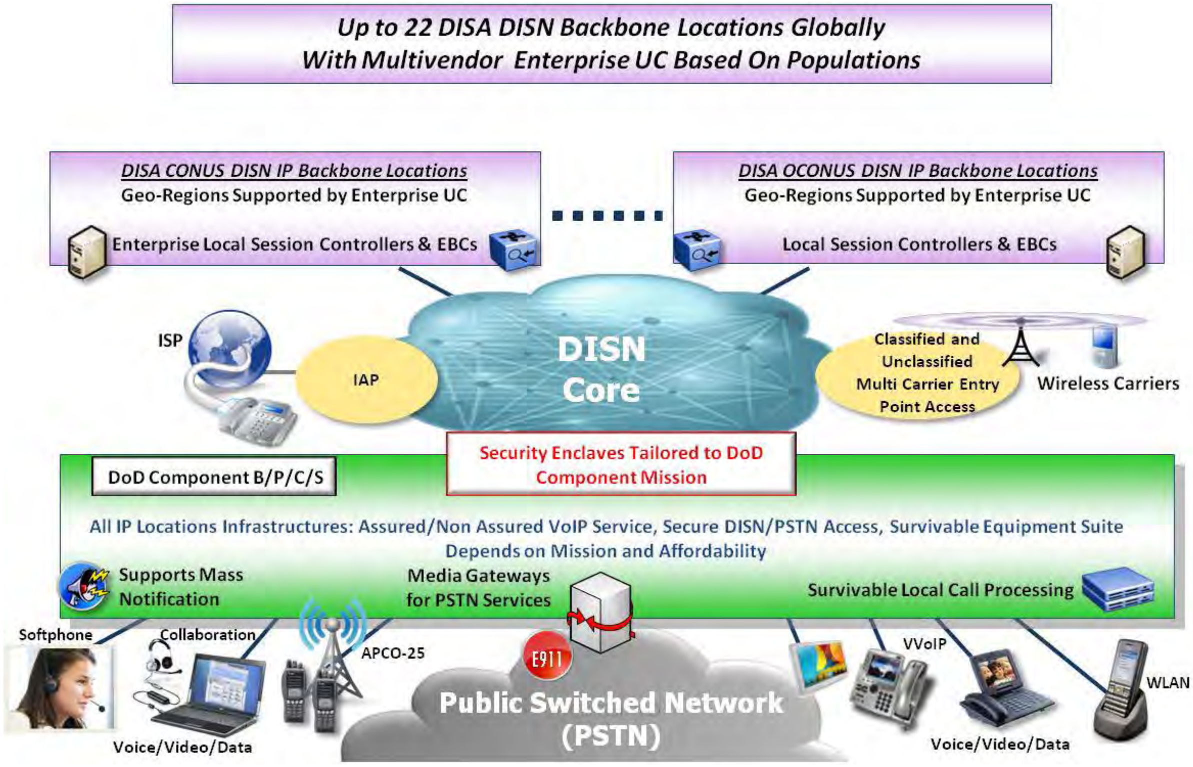
Up to 22 DISA DISN Backbone Locations Globally
With Multivendor Enterprise UC Based On Populations
DISA CONUS DISN IP Backbone Locations
Geo-Regions Supported by Enterprise UC
Enterprise Local Session Controllers & EBCs
DISA OCONUS DISN IP Backbone Locations
Geo-Regions Supported by Enterprise UC
Local Session Controllers & EBCs
ISP
IAP
DISN
Core
Classified and Unclassified Multi Carrier Entry Point Access
Wireless Carriers
Security Enclaves Tailored to DoD Component Mission
DoD Component B/P/C/S
All IP Locations Infrastructures: Assured/Non Assured VoIP Service, Secure DISN/PSTN Access, Survivable Equipment Suite
Depends on Mission and Affordability
Supports Mass Notification
Media Gateways for PSTN Services
Survivable Local Call Processing
Softphone
Collaboration
APCO-25
E911
Public Switched Network
(PSTN)
VVoIP
WLAN
Voice/Video/Data
Voice/Video/Data

Figure 4. DISN Backbone Infrastructure

(2) This operational concept has the potential to provide a single IP technology footprint, offer savings in operations and maintenance (O&M) and space requirements at the DoD Component level. At the enterprise level, this operational concept provides for integration of collaboration services, directory services, and conferencing capabilities as well as potentially enhancing NetOps situational awareness and improving end-to-end network performance.

d. Operational Construct for UC NetOps. Figure 5 defines the operational construct for UC NetOps based on the USCYBERCOM/USSTRATCOM-approved DISN UC CONOPS (Reference (f)).

(1) USCYBERCOM shall receive UC network situational awareness from DoD Component Network Operations and Security Centers (NOSCs) and the DISA Network Operation Center (NOC) infrastructure, and provide Operational Directive Messages to the DoD Components to meet mission needs. DISA and the other DoD Components shall be responsible for end-to-end UC network management, through the DISA NOC infrastructure and DoD Component NOSCs through exchange of information on end-to-end situational awareness and performance, to include quality of service, faults, configuration, administration, performance, and security.

(2) The DISA NOC infrastructure shall oversee the DISN backbone infrastructure and DISA enterprise UC.

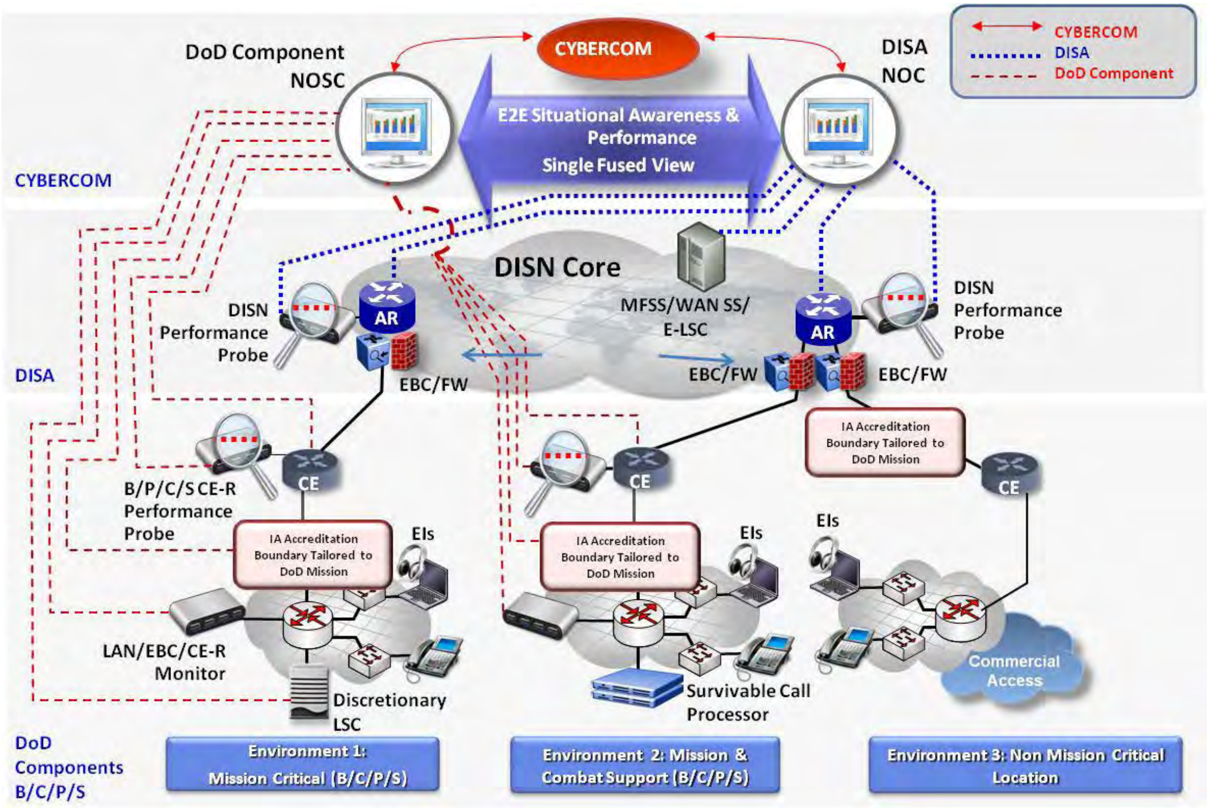
CYBERCOM
DISA
DoD Component
DoD Component NOSC
CYBERCOM
DISA NOC
E2E Situational Awareness & Performance Single Fused View
CYBERCOM
DISN Core
MFSS/WAN SS/ E-LSC
DISN Performance Probe
AR
EBC/FW
AR
EBC/FW
EBC/FW
DISN Performance Probe
DISA
IA Accreditation Boundary Tailored to DoD Mission
CE
CE
CE
B/P/C/S CE-R Performance Probe
IA Accreditation Boundary Tailored to DoD Mission
EIs
IA Accreditation Boundary Tailored to DoD Mission
EIs
EIs
LAN/EBC/CE-R Monitor
Discretionary LSC
Survivable Call Processor
Commercial Access
DoD Components B/C/P/S
Environment 1: Mission Critical (B/C/P/S)
Environment 2: Mission & Combat Support (B/C/P/S)
Environment 3: Non Mission Critical Location

Figure 5. Operational Construct for UC NetOps

(3) The DoD Component NOSCs (i.e., MILDEP and supported COCOM) shall oversee respective regional and Base/Post/Camp/Station (B/P/C/S) infrastructures supporting UC, delivered to the edge infrastructures and end devices. DoD Component B/P/C/S UC infrastructures may be tailored to meet respective mission needs for the three environments shown in Figure 5 and described in Sections 4.f.(1), 4.f.(2), and 4.f.(3).

(4) The DISA NOC and DoD Component NOSCs and associated network engineers shall collaborate on location, capabilities and network monitoring information requirements to minimize overlaps and duplication of monitoring probe capabilities and information exchange to provide end-to-end situational awareness and performance, to include quality of service, faults, configuration, administration, performance, and security.

e. Organizational Relationships/Responsibilities. Figure 6 defines the organization relationships among the UC key stakeholders consisting of the DoD CIO, Joint Staff, DISA, and the DoD Components over the life cycle of UC, from acquisition to operations to sustainment until retirement. The DoD CIO is responsible for UC policy, requirements, and overarching planning documents. The notional governance structure for UC is established in Reference (a). Final governance structure for UC implementation shall be determined when Secretary of Defense reorganization efficiencies initiatives are complete. The Joint Staff is responsible for developing and issuing UC implementing instructions. DISA is responsible for UC enterprise funding, engineering, acquisitions, operations, maintenance, and sustainment associated with the DISN backbone and edge service provider (i.e., ELSC functionality for enterprise UC). Additionally, DISA shall provide a Blanket Purchase Agreement (BPA) for the other DoD

Components to use to acquire edge infrastructure UC APL products. The use of the DISA BPA is recommended by all DoD Components. DoD Components are responsible for edge infrastructure funding, engineering, acquisitions, and operations.

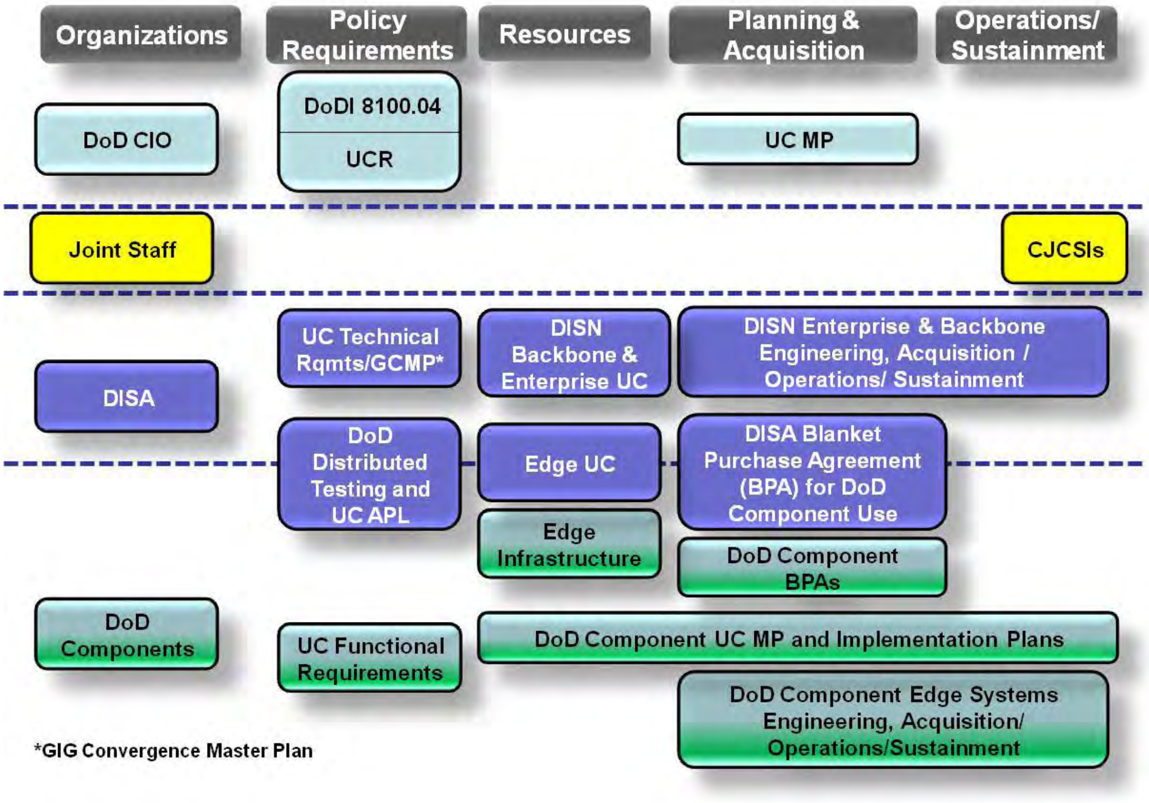
Organizations
Policy Requirements
Resources
Planning & Acquisition
Operations/ Sustainment
DoD CIO
DoDI 8100.04
UCR
UC MP
Joint Staff
CJCSIs
UC Technical Rqmts/GCMP*
DISN Backbone & Enterprise UC
DISN Enterprise & Backbone Engineering, Acquisition / Operations/ Sustainment
DISA
DoD Distributed Testing and UC APL
Edge UC
DISA Blanket Purchase Agreement (BPA) for DoD Component Use
Edge Infrastructure
DoD Component BPAs
DoD Components
UC Functional Requirements
DoD Component UC MP and Implementation Plans
DoD Component Edge Systems Engineering, Acquisition/ Operations/Sustainment
*GIG Convergence Master Plan

Figure 6. Organizational Relationships/Responsibilities

f. System Interfaces. Figure 7 depicts system interfaces between the DISN backbone and the DoD Components' edge infrastructures to deliver UC to end users. The functional requirements, performance objectives, and technical specifications needed for the initial deployment phase for assured, secure, and interoperable UC using multiple vendor products are contained in Reference (d). UC transport will be primarily provided by the DISN Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) (for unclassified services) and by the DISN Secret Internet Protocol Router Network (SIPRNet) (for classified services). A key concept depicted in Figure 7, for tailoring UC implementations in DoD, is based on three organizational mission environment types. A location's final recommended architecture will be based on the aggregate of tenant organizations' mission environments at a given location. The three mission environments are:

(1) Environment 1: Mission Critical (B/P/C/S)

(a) Organizations with mission sets that dictate, under normal conditions, access to all UC services, and in the event the location is disconnected from the DISN, require all basic UC services including intrabase precedence calling capability, external commercial services available to all users, and E911 service. Examples include a combat support unit or operational flying wing.

(b) The same as paragraph 4.f.(1)(a), but in tactical deployed locations such as Afghanistan or Iraq with increased level of local management.

(2) Environment 2: Mission and Combat Support (B/P/C/S). Organizations with mission sets that dictate, under normal conditions, access to all UC services, and in the event the location is disconnected from the DISN, require limited voice-only services, and limited external commercial services (E911 and external dial tone). An example of this would be a training unit or an administrative center.

(3) Environment 3: Non Mission Critical Locations. Organizations with mission sets that do not require significant voice services or external commercial services (E911, and external dial tone) in the event the location is disconnected from the DISN. An example would be a small administrative function (e.g., recruiting office). In this case, E911 and other services could be provided by other means (e.g., cellular, leased services).

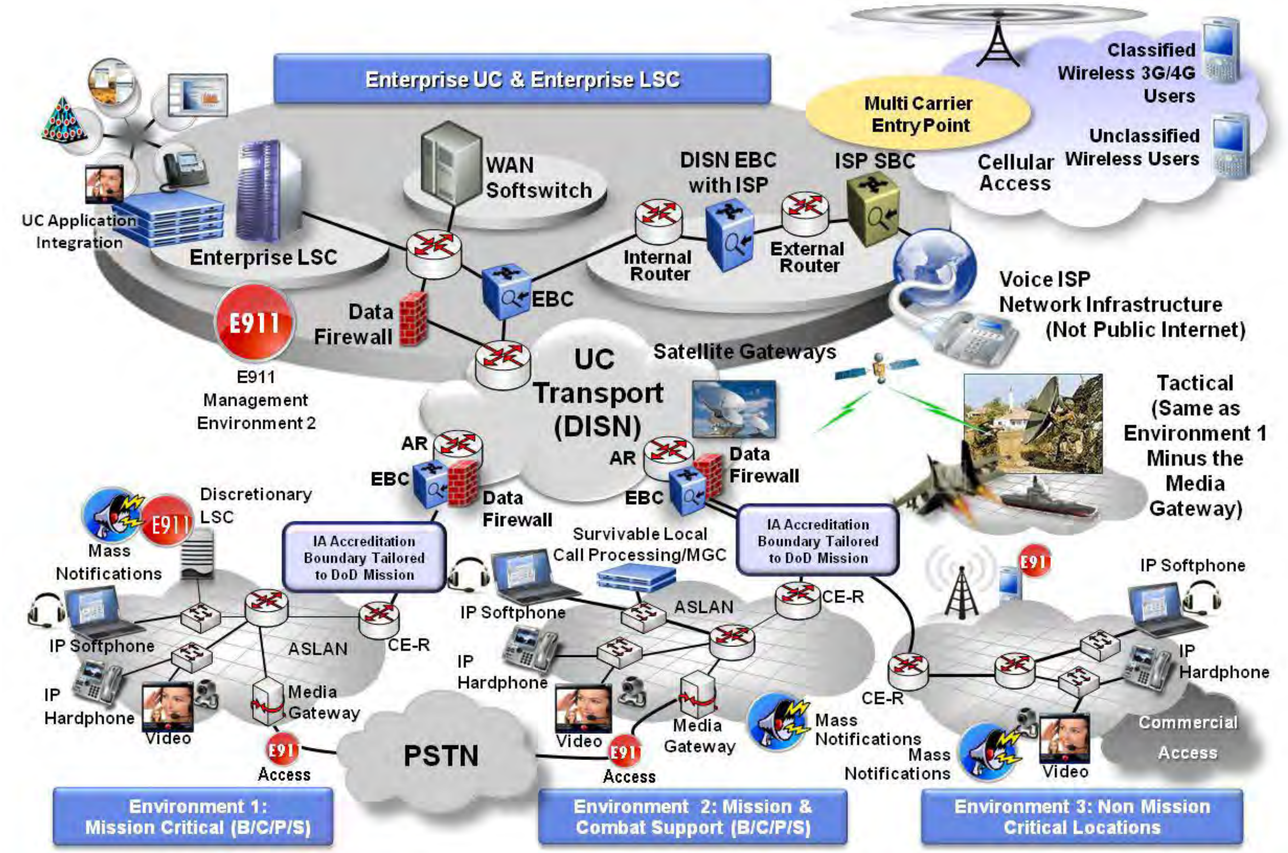
Enterprise UC & Enterprise LSC
Multi Carrier Entry Point
Classified Wireless 3G/4G Users
Unclassified Wireless Users
Cellular Access
UC Application Integration
Enterprise LSC
WAN Softswitch
DISN EBC with ISP
ISP SBC
Internal Router
External Router
Voice ISP Network Infrastructure (Not Public Internet)
E911
Data Firewall
EBC
UC Transport (DISN)
Satellite Gateways
E911 Management Environment 2
Tactical (Same as Environment 1 Minus the Media Gateway)
AR
EBC
Data Firewall
AR
Data Firewall
EBC
Discretionary LSC
E911
Mass Notifications
IA Accreditation Boundary Tailored to DoD Mission
Survivable Local Call Processing/MGC
IA Accreditation Boundary Tailored to DoD Mission
CE-R
IP Softphone
IP Softphone
ASLAN
IP Softphone
ASLAN
CE-R
IP Hardphone
IP Hardphone
IP Hardphone
Media Gateway
Video
E911
Access
PSTN
Video
E911
Access
Media Gateway
Mass Notifications
CE-R
Mass Notifications
Commercial Access
Video
Environment 1: Mission Critical (B/C/P/S)
Environment 2: Mission & Combat Support (B/C/P/S)
Environment 3: Non Mission Critical Locations

Figure 7. Systems Interfaces

g. Functional Requirements, Performance Objectives, Standards, and Technical Specifications. The standards for UC implementation are based on commercial standards mandated in the DoD IT Standards Registry (DISR) and Data Services Environment, augmented as necessary, to meet DoD security requirements and to achieve multi-vendor interoperable solutions. Commercial standards will be employed for non-assured services, as appropriate. Reference (d) captures appropriate standards from the DISR and specifies the functional requirements, performance objectives, standards, and technical specifications for DoD networks that support UC.

5. UC IMPLEMENTATION STRATEGY. The UC implementation strategy supports Reference (e) goals and corresponding enterprise UC initiatives.

a. Implementation Strategy Precepts. The UC implementation is based on the following precepts:

(1) Drive technology insertion through a common UC operational framework.

(2) Transition to UC using implementation phases defined by each DoD Component, as specified in respective DoD Component implementation plans. DISA and the other DoD Components shall collaboratively integrate these implementation phases to maintain consistency and integrity of the UC operational framework, and to manage overall DoD UC risks.

(3) Employ prototype, preproduction, multi-vendor, and UC Pilot test and evaluation activities to ensure products are interoperable, secure, and NetOps compliant.

(4) Use competitive multi-vendor approved products based on common user requirements and listed on the DoD UC APL.

(5) Ensure Quality of Service (QoS) is available end-to-end, independent of technology employed, for non-assured/assured UC.

(6) Reduce the Defense Red Switch Network (DRSN) footprint by revalidating user requirements, migrating users, as appropriate, to classified DISN voice services such as Voice over Secure Internet Protocol (VoSIP), investing in an IP capable DRSN, and enabling gateways among DoD classified voice networks.

(7) Provide UC across DoD and commercial networks using commercial standards, as appropriate.

(8) Implement end-to-end UC at a pace consistent with respective DoD Component mission requirements and available resources. DoD Components shall coordinate with DISA on UC implementation schedules to ensure synchronization across the DoD enterprise.

(9) Use the DoD identity management and access control process.

b. Capabilities Synchronization. Figure 8 defines the phasing timeline goals (dependent on DoD Component mission requirements and available resources) for implementation of enterprise UC consistent with capabilities and priorities identified in Figure 3.

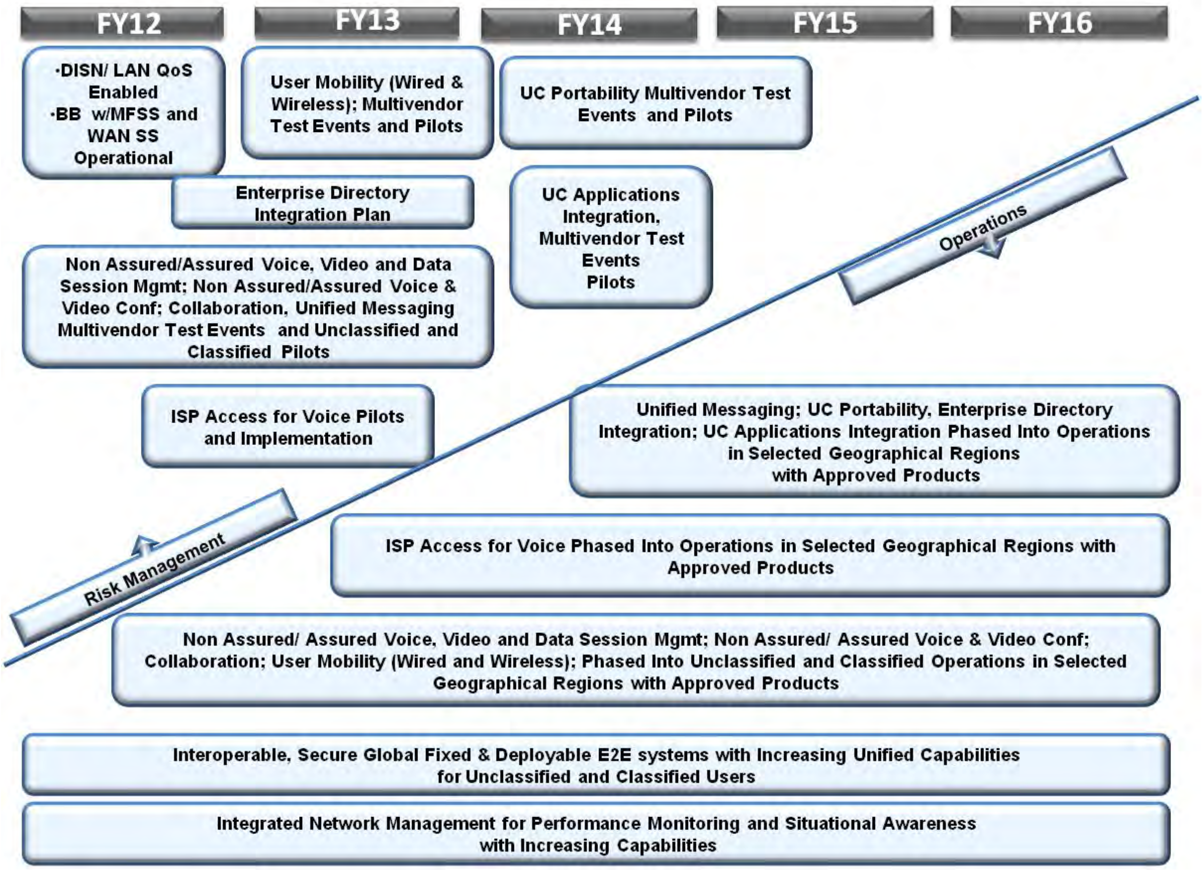
FY12
FY13
FY14
FY15
FY16
·DISN/ LAN QoS Enabled
·BB w/MFSS and WAN SS Operational
User Mobility (Wired & Wireless); Multivendor Test Events and Pilots
UC Portability Multivendor Test Events and Pilots
Enterprise Directory Integration Plan
UC Applications Integration, Multivendor Test Events Pilots
Operations
Non Assured/Assured Voice, Video and Data Session Mgmt; Non Assured/Assured Voice & Video Conf; Collaboration, Unified Messaging Multivendor Test Events and Unclassified and Classified Pilots
ISP Access for Voice Pilots and Implementation
Unified Messaging; UC Portability, Enterprise Directory Integration; UC Applications Integration Phased Into Operations in Selected Geographical Regions with Approved Products
Risk Management
ISP Access for Voice Phased Into Operations in Selected Geographical Regions with Approved Products
Non Assured/ Assured Voice, Video and Data Session Mgmt; Non Assured/ Assured Voice & Video Conf; Collaboration; User Mobility (Wired and Wireless); Phased Into Unclassified and Classified Operations in Selected Geographical Regions with Approved Products
Interoperable, Secure Global Fixed & Deployable E2E systems with Increasing Unified Capabilities for Unclassified and Classified Users
Integrated Network Management for Performance Monitoring and Situational Awareness with Increasing Capabilities

Figure 8. Capabilities Synchronization

c. Critical Dependencies. Table 1 identifies the critical dependencies for implementing UC in DoD.

Table 1. Critical Dependencies

Capability	**Critical Dependencies**
Deploy all required enterprise UC and ELSC capabilities	• Multifunction Softswitches (MFSSs)/Wide Area Network Softswitches (WAN SSs) deployed globally • Maturity of vendor's commercial products • Successful ELSC multi-vendor test events • Successful UC pilot T&E events • Availability of enterprise UC products on the DoD UC APL
Deploy all edge capabilities	• Edge infrastructure LANs (wired or wireless) consistent with the UCR • Maturity of vendor's commercial ELSC products • Successful multi-vendor test events • Successful UC pilot T&E events • Availability of edge UC products on the DoD UC APL
Implement Non-assured/assured Voice,	• Vendor's capability to augment existing LSCs with

Video, and Data Session Management	enterprise UC and to address E911 and Mass Notification • Successful lab testing of products • Successful UC pilot T&E events • Update to UCR • Availability of products on the UC APL
Non-assured/assured Voice and Video Conferencing	• Vendor's capability to augment existing commercial voice and video conferencing to meet interoperability and IA requirements • Successful lab testing of products • Successful UC pilot T&E events • Update to UCR • Availability of products on the UC APL
Implement Collaboration	• Vendor's capability to augment existing commercial applications for XMPP interoperable IM/Chat/Presence services and to meet IA requirements • Successful lab testing of products • Successful UC pilot T&E events • Update to UCR • Availability of products on the UC APL
Implement User Mobility (wired and wireless)	• Vendor's capability to augment existing commercial applications for enterprise UC and to meet IA requirements • Successful lab testing of products • Successful UC pilot T&E events • Update to UCR • Availability of products on the UC APL
Implement ISP Access for voice	• Successful UC pilot T&E events • Availability of Edge Boundary Controller (EBC) products with Intrusion Detection System (IDS) (on the DoD UC APL)
Implement Unified Messaging	• Vendor's capability to augment existing commercial applications to meet IA requirements • Successful lab testing of products • Successful UC pilot T&E events • Update to UCR • Availability of products on the UC APL
Implement UC Portability	• Successful collaboration with the DISA and DoD Component Identity Management, Identity authentication efforts • Successful lab testing of products • Successful UC pilot T&E events • Update to UCR • Availability of products on the UC APL
Implement Enterprise Directory Integration	• Successful collaboration with the DoD Component directory efforts and the DoD JEDS program to finalize directory architecture • Successful lab testing of products • Successful UC pilot T&E events

	• Update to UCR • Availability of products on the UC APL
Implement UC Applications Integration	• Successful collaboration with the DoD Component efforts and the DISA Net-Centric Enterprise Services (NCES) program to address the mission and business applications integration with the LSCs • Successful lab testing of products • Successful UC pilot T&E events • Update to UCR • Availability of products on the UC APL

d. Enterprise UC Implementation

(1) Current through FY 12 UC Implementations. UC are currently provided in a decentralized manner as follows:

(a) Time-Division Multiplexing (TDM)-based Defense Switched Network (DSN), with unclassified Voice over IP (VoIP) over non-assured/assured services LANs (NAS/AS LANs) to the local circuit switch using the TDM transport over the DISN.

(b) TDM-based DRSN with multilevel secure services using TDM transport over the DISN.

(c) VoSIP with SECRET level best effort services using the SIPRNet.

(d) DISN Video Services (DVS) Video Teleconferencing (VTC) services via a mixture of DSN Integrated Services Digital Network (ISDN) services and limited DVS video over IP for both unclassified and SECRET level services.

(e) Data services provided over NIPRNet and SIPRNet.

(f) Standardized Tactical Entry Point (STEP)/Teleport, and other DoD Component satellite gateways.

(g) Tactical capabilities using various gateways to connect to the DSN, or gateways that connect to tactical VoIP services.

(h) Circuit switched based services shall begin migrating to IP-based non-assured/assured services over DoD Component ASLANs/Intranets, and UC transport using products from the DoD UC APL (except DRSN, which is discussed in paragraph 5.f). During this implementation timeframe, both converged and non-converged UC shall be provided by TDM/IP hybrid technologies. The VoSIP, DVS, STEP/Teleport, and deployable programs shall upgrade respective infrastructures using products from the DoD UC APL. The phase out of circuit switched technologies shall be based on the following individual conditions:

1. New Circuit Switched Products. New circuit switched products shall no longer be tested and certified for placement on the UC APL as of January 2011.

2. Existing UC APL Circuit Switched Products. Existing circuit switched products on the UC APL may be purchased until certification expires and removed from the APL.

3. Installed UC Circuit Switched Products. Existing circuit switched products already installed, UC APL products procured before the UC APL expiration date, or on the Retired UC APL List may remain until business case or mission need dictates replacement, or vendor is no longer willing to support. Continued testing and certification for software patches is allowed for these components while in use, however this testing and certification shall not result in renewed UC APL status.

(i) During this period, DISA shall deploy MFSSs and WAN SSs, allowing DoD Components to implement UC employing IP while maintaining backward interoperability with the remaining circuit-switch/TDM technologies. DISA's enterprise voice and video services, with collaboration capabilities (IM, presence, and chat), shall be evaluated during UC Pilot Spiral 2 and shall begin operations in select geographic regions during this timeframe. Figure 9 illustrates the potential 22-sites for potential MFSS and WAN SSs global deployments.

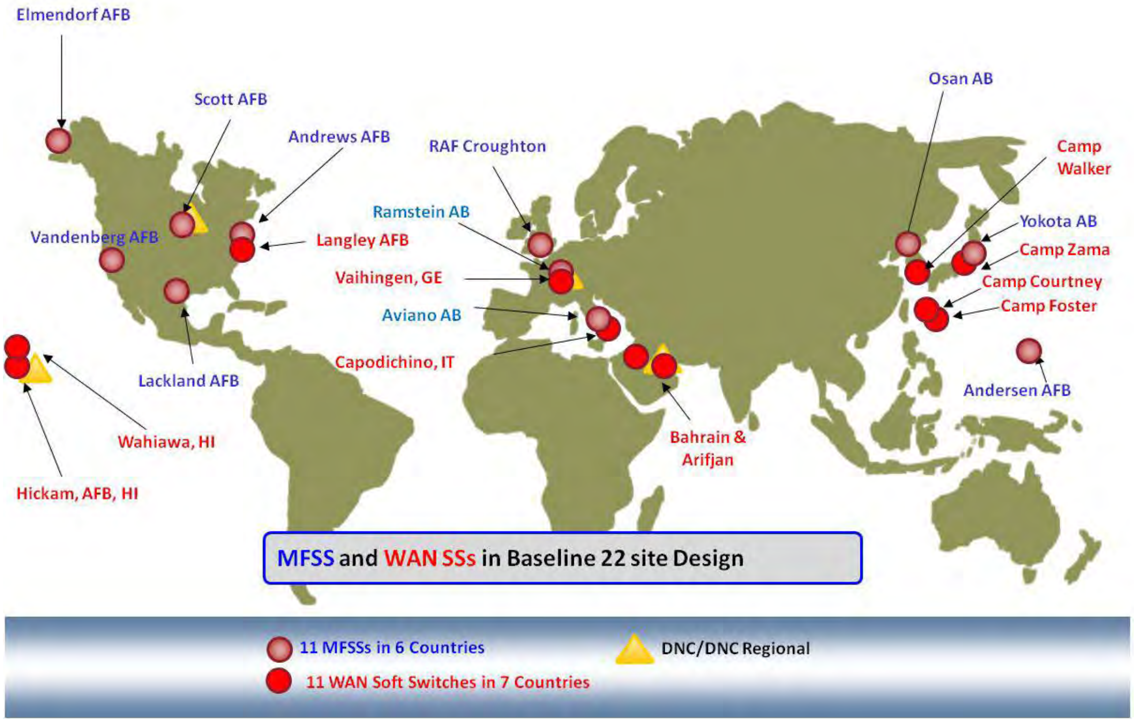

Figure 9. Potential 22 MFSS/WAN SSs Global Sites

These sites were chosen based on the UC operational framework; survivability; availability; network performance; and maintenance and operation support to include existing backbone locations with intra-service support agreements with DISA. A nominal set of 18 sites shall be considered for initial deployments, based on geographic region and Combatant Commander (CCDR) considerations. Locations may be changed based on operational needs for survivability, redundancy, diversity, and user population. The operational dates for these sites are depicted in Table 2.

(j) DISA shall introduce UC Spiral 2 pilots in OCONUS and CONUS to validate the UC operational framework.

Table 2. Operational Dates

Geographic Region	DoD Component	Site	SS and ELSC	Operational Dates
CONUS	Air Force	Lackland Air Force Base (AFB), Texas	MFSS	Operational
CONUS	Air Force	Scott AFB, Illinois	MFSS	Operational
CONUS	Air Force	Andrews AFB, Maryland	MFSS	Operational
CONUS	Air Force	Vandenberg AFB, California	MFSS	Operational
EUCOM	Air Force	Ramstein, Germany	MFSS	Operational
EUCOM	Air Force	Molesworth, United Kingdom	MFSS	Operational
EUCOM	Air Force	Aviano, Italy	MFSS	Operational
PACOM	Air Force	Yokota, Japan	MFSS	Operational
PACOM	Air Force	Andersen AFB, Guam	MFSS	Operational
PACOM	Air Force	Elmendorf AFB, Alaska	MFSS	Operational
PACOM	Air Force	Osan, Korea	MFSS	FY 11
PACOM	Army	Camp Walker, Korea	WAN SS	FY 11
PACOM	Marines	Camp Foster, Okinawa	WAN SS	FY 11
PACOM	Navy	Wahiawa, Hawaii	WAN SS	FY 11
PACOM	Air Force	Hickam AFB, Hawaii	WAN SS	FY 11
EUCOM	Army	Vaihingen, Germany	WAN SS	FY 11
EUCOM	Air Force	RAF Croughton (from Molesworth), United Kingdom	MFSS	FY 12
CENTCOM	Navy	Manama (5th Fleet), Bahrain	WAN SS	FY 12
CENTCOM	Army	Camp Arifjan, Kuwait	WAN SS	FY 12
PACOM	Army	Camp Zama, Japan	ELSC	FY 12
PACOM	Marines	Camp Courtney, Okinawa	ELSC	FY 12
EUCOM	Navy	Capodichino, Italy	ELSC	FY 12
CONUS	Air Force	Langley AFB, Virginia	ELSC	FY 12

(2) FY 12 through FY 16 UC Implementation. The enterprise UC implementation strategy shall replace costly circuit switched technologies with IP-based capabilities to achieve potential cost avoidance/reduction, at a pace that is affordable and mission effective for the DoD Components. This strategy shall be implemented as follows:

(a) DISA shall:

1. Develop, in collaboration with the other DoD Components, an initial Business Case Analysis (BCA) for an end-to-end implementation of the UC within 180 days of issuance of the UC MP for submission to CAPE for review and approval. The BCA shall provide cost analysis and budgetary planning for implementation of enterprise-wide voice, video, and data services.

2. Develop, in collaboration with the other DoD Components, an end-to-end DoD Enterprise UC Implementation Plan within 120 days of issuance of the UC MP.

3. Establish, in coordination with the other DoD Components, the priority for geographic regions to implement enterprise UC pilots and begin enterprise UC operations.

4. Continue to refine, in coordination with the other DoD Components, the NetOps concept of operations, to include Tactics, Techniques, and Procedures (TTPs), for approval by USCYBERCOM/USSTRATCOM.

5. Conduct multi-vendor test events and deploy UC pilots in selected geographic regions to support enterprise UC implementation.

6. Update the UCR, and test and certify enterprise UC products for placement on the DoD UC APL. Ensure commercial, multi-function mobile device functional, performance, and technical requirements, to support full access to unsecure and secure applications, are reflected in the UCR.

7. Fund, acquire, deploy, operate and sustain unclassified and classified enterprise UC (e.g., DISN backbone, ELSCs, MCEPs, etc.) for geographic regions in the priority identified in the DISA UC Implementation Plan.

8. Establish a BPA, within 180 days of issuance of the UC MP, for use by all DoD Components to acquire, at volume discounts, the UC APL products needed for edge UC infrastructure implementation.

9. Upgrade the DISN to meet QoS and network requirements, as specified in the Reference (d).

(b) The DoD Components shall:

1. Develop, in collaboration with DISA, the respective DoD Component UC Implementation Plans within 120 days of issuance of the UC MP.

2. Establish, in coordination with DISA, the priority for geographic regions to implement enterprise UC pilots and begin enterprise UC operations.

3. Continue to refine, in coordination with DISA, the Enterprise NetOps concept of operations, to include TTPs, for approval by USCYBERCOM and USSTRATCOM.

4. Participate in UC pilots in selected geographic regions to support enterprise UC.

5. Use DoD UC APL for purchase of all UC products.

6. Fund, acquire, deploy, operate, and sustain Component UC products, for geographic regions in the priority identified in the DISA and DoD Component UC Implementation Plans. Either DISA or other DoD Components may provide enterprise UC in a geographic region.

7. Use DISA's UC APL BPA, at DoD Component's discretion, as the preferred BPA, assuming it is the lowest cost, for acquisition of UC APL products needed for edge infrastructure implementation.

8. Upgrade networks to meet QoS and LAN requirements, as specified in the Reference (d).

e. Implementation Schedule and Risks. Figure 10 defines the schedules for UC implementation. There are four key elements of implementation: planning, DISN backbone infrastructure, NetOps, and the DoD Component edge. Critical milestones for each FY are shown, associated with each of the four implementation elements.

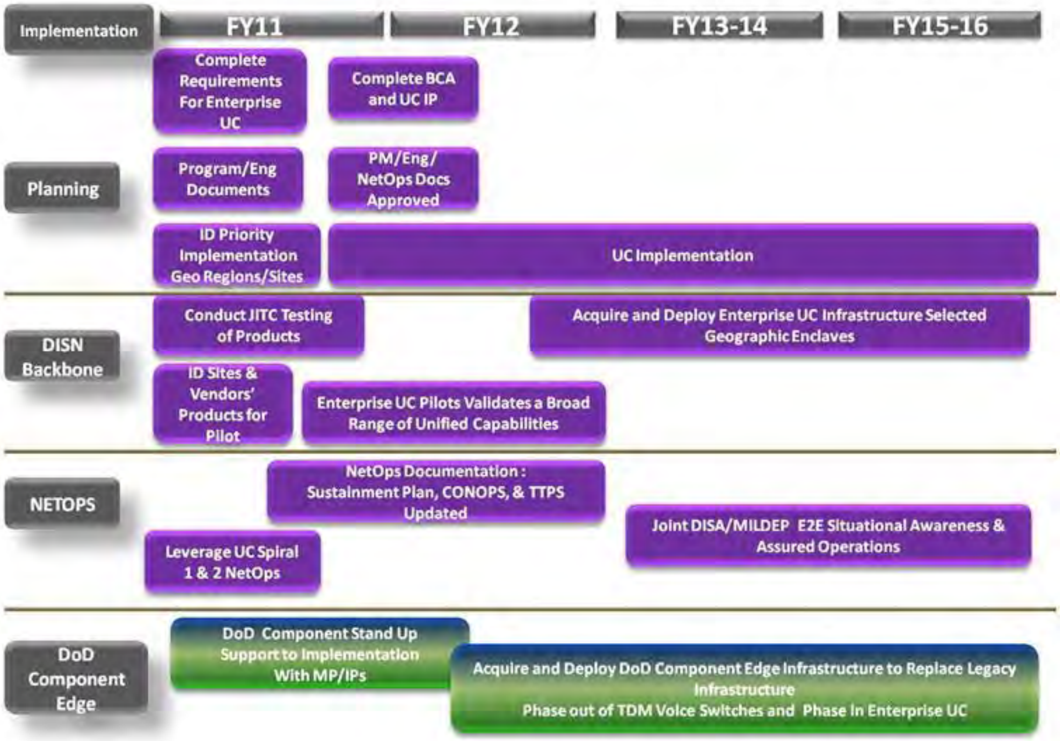
Implementation
FY11
FY12
FY13-14
FY15-16
Complete Requirements For Enterprise UC
Complete BCA and UC IP
Planning
Program/Eng Documents
PM/Eng/ NetOps Docs Approved
ID Priority Implementation Geo Regions/Sites
UC Implementation
DISN Backbone
Conduct JITC Testing of Products
Acquire and Deploy Enterprise UC Infrastructure Selected Geographic Enclaves
ID Sites & Vendors' Products for Pilot
Enterprise UC Pilots Validates a Broad Range of Unified Capabilities
NETOPS
NetOps Documentation : Sustainment Plan, CONOPS, & TTPS Updated
Joint DISA/MILDEP E2E Situational Awareness & Assured Operations
Leverage UC Spiral 1 & 2 NetOps
DoD Component Edge
DoD Component Stand Up Support to Implementation With MP/IPs
Acquire and Deploy DoD Component Edge Infrastructure to Replace Legacy Infrastructure
Phase out of TDM Voice Switches and Phase In Enterprise UC

Figure 10. Enterprise UC Implementation Schedule

(1) Implementation planning starting in FY 11 includes identification of requirements for enterprise UC; preparation of program and engineering documentation; awarding contracts for the DISN backbone; and identifying DoD Component edge priorities for implementation by geographical regions, to include specific site installations.

(2) DISN backbone infrastructure implementation, starting in FY 11, includes test and evaluation of enterprise UC products, identifying vendor products and sites for enterprise UC pilots. From FY 12 to FY 16, enterprise UC pilots shall be completed; global deployment shall begin; and DISA shall acquire and deploy the DISN enterprise UC backbone infrastructure. Authorization to Operate (ATO) and Approval to Connect (ATC) processes required in Reference (a) shall be followed for operation of UC capabilities.

(3) Enterprise UC pilot implementation starts in FY 12. Based on the pilot results and the operational lessons from the UC Spirals, the UC CONOPS shall be updated and approved by USCYBERCOM/USSTRATCOM.

(4) DoD Component edge implementation planning will commence with the identification of resources and support necessary for implementation in FY 11 or FY 12 depending on available resources, mission needs, and Component priorities. Starting in FY 12, DoD Components shall support UC pilots and, as legacy technologies reach end-of-life, shall begin to procure and deploy component-specific UC APL products and infrastructures based on resource availability and approved Cost Assessment and Program Evaluation (CAPE) UC BCA.

(5) Table 3 defines risks and mitigations for enterprise UC implementation.

Table 3. Implementation Risks and Mitigations

RISK Category: Assessment of ability to meet performance requirements, security risks, and associated mitigation plan to address risks	
RISKS	**MITIGATION**
• Limited vendors capable of providing enterprise UC	Schedule multi-vendor test events to evaluate vendor's commercial enterprise capabilities, and then expand to assured/non assured service test events and UC pilots and update the UCR in FY 12
• DISN enterprise backbone not fully deployed and operational by end of FY 12 for prioritized geographic regions	Multi-vendor test event on enterprise UC products and UC pilots fully supported during end of FY 12. Joint prioritization of geographic regions and sites based on number of TDM switches and vendor product readiness by early of FY 12
• UC operational framework unable to meet full range of user requirements	Employ the UC risk management process based on DoDI 8100.04 defined UC governance, UCR , distributed testing, and UC pilots
• Centralization of services using ELSCs may result in increased bandwidth requirements which offset potential enterprise cost savings.	DoD Component and DISA collaborative traffic engineering and operational pilots to evaluate potential increased bandwidth requirements and associated cost implications
• DoD Component base infrastructure not engineered to meet UCR performance objectives.	DoD Component perform network engineering study (to assess compliance with UCR packet loss, latency and jitter requirements) and upgrade network infrastructure as required

Risk Category: Assessment of ability to meet planned schedules	
RISKS	**MITIGATION**
• CAPE does not approve BCA per schedule	DISA submit BCA in response to DoD IT Efficiencies Initiative
• Inability to synchronize DoD Component UC implementation schedules	UC Steering Group to integrate DoD Component UC implementation plans
• DoD Components unable to establish qualified implementation teams and prepare their master plan/ implementation plans to implement UC per UC MP timeline	DISA meet with DoD Components in FY 12 and establish work groups as needed
• DoD Component installation sites not ready by scheduled implementation date	DoD Component senior direction to Component site locations. DoD Components establish core team of PM, engineer, IA expert, and NetOps expert and draft respective implementation plans. Joint prioritization of geographic regions and sites based on number of TDM switches and vendor product readiness by end of FY 11
• Inadequate IT staff skill sets for UC implementation at each site	DoD Components leverage on-going UC pilots lessons learned. When requested, DISA provide partial or complete managed services
• ATO and ATC not achieved at each site on the schedule	DoD Components are required to: -- Direct DAA/CAs to ensure UC efforts receive priority in executing ATO and ATC accreditation decisions -- Provide IA and IP technically qualified staff in support of UC acquisitions and operations -- Use and accept reciprocity for accreditation and certification of decisions on UC products
• DISA BPA not available for edge site enterprise infrastructure acquisition	DoD Components using DISA BPA , if most mission/cost effective, in FY 12
Risk Category: Assessment of resource requirements to meet the UC migration strategy	
RISKS	**MITIGATION**
• DISA resources insufficient for implementing enterprise backbone infrastructure	DISA funding for enterprise UC services and infrastructure committed in FY 12
• DoD Component resources insufficient for implementing enterprise edge infrastructure	DoD Components are required to use: -- Existing network modernization and technology refreshment resources for implementing enterprise UC in FY 12/13 -- UC MP to influence POM FY 14 submissions and beyond for implementing UC

• Initial cost estimates inaccurate	DoD Components are required to: -- Leverage DISA UC Enterprise RFI to improve cost models -- Collaborate on cost models, vendor discussions, and update models for consistency across DoD -- Conduct multi-vendor competition for UC acquisitions

f. Enterprise UC Secure Voice Services

(1) Secure voice services support critical command and control capabilities. The goal for secure voice services is to ensure network connectivity and secure mobile capabilities are accessible anywhere, at any time in the network. The Joint Staff shall validate secure voice requirements.

(2) Future enterprise UC secure voice shall fully exploit IP technologies, meet DoD mission needs for Multi Level Security (MLS), and consider the following implementation precepts:

(a) Reduce the DRSN footprint and increase the use of VoSIP, recognizing the following constraints:

1. The DRSN provides some unique capabilities (MLS, C2 large conferencing, and tailored conference management capabilities) – not supported in IP today.

2. Secure voice capability can be supported by VoSIP as a means for SECRET voice only and DRSN long locals for higher security voice requirements.

(b) Enable DRSN switches with IP technologies to eliminate the need for multiple gateways.

(c) Develop interconnects across multiple security boundaries for DoD and NSA secure voice IP networks.

(3) To implement IP-enabled secure voice services:

(a) Joint staff shall determine and validate/revalidate secure voice requirements.

(b) DISA shall:

1. In coordination with DoD CIO, Joint Staff, and other DoD Components, collect and evaluate secure voice requirements, and provide recommendations to the Joint Staff.

2. In coordination with the Joint Staff and other DoD Components, provide a Plan of Action and Milestones (POA&M) to re-engineer and optimize secure voice services for an IP-enabled environment.

3. Identify resource requirements, engineering, and implementation plans for MLS capabilities using IP technologies.

4. In coordination with NSA, develop the secure voice services component of the UC operational framework to support the next generation of secure multi-function mobile devices.

5. Implement interconnects across multiple security boundaries for DoD and NSA secure voice IP networks.

6. Upgrade the DISN to meet QoS and network requirements, as specified in the Reference (d).

(c) DoD Components shall:

1. Collect, evaluate, and recommend Joint Staff validation/revalidation of secure voice requirements.

2. Support DISA development of a POA&M to re-engineer and optimize secure voice services for an IP-enabled environment in FY 12.

3. In coordination with NSA and DISA, develop the requirements for, and support the next generation of secure multi-function mobile devices.

4. Support DISA development of interconnects across multiple security boundaries for DoD and NSA secure voice IP networks.

5. Upgrade DISN edge to meet QoS and network requirements, as specified in the Reference (d).

6. RESOURCE PLANNING AND RESPONSIBILITIES. To focus limited DoD Component resources, existing circuit switch technologies shall be replaced with more capable, cost effective, and sustainable enterprise UC APL products compliant with the UC operational framework and UCR. For the period FY 12-16, existing network infrastructure modernization and technology refresh funding shall be used to implement enterprise UC by all DoD Component. DISA and the other DoD Components shall execute the following resource responsibilities:

a. DISA shall:

(1) In collaboration with the other DoD Components, lead the development of a BCA to meet the end-to-end requirements of the UC operational framework for the DoD CIO Executive Board's assessment, and the Department's decision-making processes. The BCA shall provide a full range of voice capabilities from central locations that fully leverage the DISN and IP technologies. The BCA shall aggregate the implementation of UC on DISN backbone, DISN common and edge UC, and incorporate each DoD Component's BCA for UC implementation. This approach shall avoid cost duplication for services, operations and maintenance (O&M), network operations, sustainment, and information assurance at DoD locations worldwide for a lower total cost of ownership. The Director, CAPE, shall review and approve this BCA.

(2) Based on the CAPE-approved BCA, fund unclassified and classified enterprise UC per the priority identified in the DISA UC Implementation Plan.

b. DoD Components shall:

(1) In collaboration with DISA, support and provide input in the development of a BCA to meet the end-to-end requirements of the UC operational framework.

(2) Based on the CAPE-approved BCA, prioritize existing FY 12/13 UC network infrastructure modernization and technology refreshment investments and operations and maintenance budgets to implement UC, consistent with respective DoD Component's missions and resources.

(3) Based on the CAPE-approved BCA, identify FY 14 POM investments, operations, and sustainment funding needed to implement UC within respective DoD Components' implementation plans.

REFERENCES

(a) DoD Instruction 8100.04, “DoD Unified Capabilities (UC),” December 9, 2010
(b) DoD Directive 5000.01, “The Defense Acquisition System,” May 12, 2003
(c) DoD Instruction 5000.02, “Operation of the Defense Acquisition System,” December 8, 2008
(d) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Publication, “Department of Defense Unified Capabilities Requirements,” current edition, located at http://disa.mil/ucco
(e) Secretary of Defense Memorandum, “Department of Defense (DoD) Efficiency Initiatives,” August 16, 2010
(f) Defense Information Systems Network (DISN) UC CONOPS

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AFB	Air Force Base
APL	Approved Products List
APCO	Association of Public Safety Communications Officials
AR	Aggregate Router
ASAC	Assured Services Admission Control
ASLAN	Assured Service Local Area Network
AS-SIP	Assured Services Session Initiation Protocol
BCA	Business Case Analysis
B/P/C/S	Base/Post/Camp/Station
BPA	Blanket Purchase Agreement
BRAC	Base Realignment and Closure
C2	Command and Control
CAPE	Cost Assessment and Program Evaluation
CCDR	Combatant Commander
CER	Customer Edge Router
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMS	Crisis Management System
COCOM	Combatant Command
COI	Communities of Interest
CONOPS	Concept of Operations
DCO	Defense Connect Online
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DNC	DISA NETOPS Center
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DOTS	DISN Overarching Technical Strategy

DRSN	Defense Red Switch Network
DSS	DISN Subscription Service
DTEP	DISN Technical Evolution Plan
DVS	DISN Video Services
E2E	End-to-End
EBC	Edge Boundary Controller
EI	End Instrument
ELSC	Enterprise Local Session Controller
FY	Fiscal Year
GIG	Global Information Grid
IA	Information Assurance
IAP	Internet Access Point
IDS	Intrusion Detection System
IM	Instant Messaging
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
JITC	Joint Interoperability Test Command
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LSC	Local Session Controller
MCEP	Multi-Carrier Entry Point
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
MILDEP	Military Department
MPLS	Multiprotocol Label Switching
NATO	North America Treaty Organization

NCP	Network Cutover Plan
NETOPS	Network Operations
NOSC	Network Operations and Security Center
NSTS	National Security Telephone System
O&M	Operations and Maintenance
PKI	Public Key Infrastructure
POM	Program Objective Memorandum
PDA	Personal Digital Assistant
PSTN	Public Switch Telephone Network
QoS	Quality of Service
SA	Situational Awareness
SATCOM	Satellite Communication
SBC	Session Border Controller
SDN	Service Delivery Node
SRTP	Secure Real-Time Protocol
STEP	Standardized Tactical Entry Point
TDM	Time-Division Multiplexing
TLS	Transport Layer Security
TNC	Theater NetOps Center
UC	Unified Capabilities
UC MP	Unified Capabilities Master Plan
UCR	Unified Capabilities Requirements
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VoSIP	Voice over Secure IP
VTC	Video Teleconferencing

VVoIP	Voice and Video over IP
WAN SS	Wide Area Network Softswitch
XMPP	Extensible Messaging and Presence Protocol

PART II. DEFINITIONS

APCO-25. A suite of standards for digital radio communications for use by federal, state/province and local public safety agencies in North America to enable communications with other agencies and mutual aid response teams in emergencies.

Assured Service. The ability of a system to optimize session completion rates for all IMMEDIATE/PRIORITY (I/P) users despite degradation because of network disruptions, natural disasters, or surges during crisis or war.

ASF. The three assured service attributes that provide for the survivability of DoD networks that support UC. These are:

assured system and network availability. Achieved through visibility and control over the system and network resources. Resources are managed and problems are anticipated and mitigated, ensuring uninterrupted availability and protection of the system and network resources. This includes providing for graceful degradation, self-healing, fail over, diversity, and elimination of critical failure points. This ASF supports user traffic during peacetime, crisis, conflict, natural disaster, and network disruptions, and possesses the robustness to provide a surge capability when needed.

assured information protection. Applies to information in storage, at rest, and passing over networks, from the time it is stored and catalogued until it is distributed to the users, operators, and decision makers. Secure end devices shall be used for the protection of classified and sensitive information being passed to ensure its confidentiality, integrity, and authentication. DoD networks that support UC shall be configured to minimize attacks on the system that could result in denial or disruption of service.

assured information delivery. The requirement that DoD networks that support UC have the ability to optimize session completion rates despite degradation due to network disruptions, natural disasters, or surges during crisis or war.

AS-SIP. A session signaling protocol consisting of a defined set of Session Initiation Protocol signaling standards and incorporating Department of Defense Assured Service functionality.

Centralized EBC. An EBC that protects multiple enclaves or locations.

DISA NETOPS Center (DNC). Provides general support to the day-to-day technical operation, control, and management of the CONUS portions of the DISN. The DNC-CONUS conducts backbone NetOps, tactical DISN extension via Standard Tactical Entry Point (STEP) and Teleport mission support, provisioning of provided services, network engineering, circuit implementation, and inter-theater connectivity.

DNC Regional. Provides support to its Theater Network Control Center (TNCC) or supporting COCOM, ensuring the effective operation and defense of the DISN networks within the theater. A DNC Regional may also provide day-to-day technical operation, control, and management of portions of the DISN that support global operations, but are not assigned to a COCOM. DISA has four DNC-Regionals supporting four COCOMs in the respective theaters: DNC-Europe/Africa, DNC-Central, DNC-Pacific, and DNC-North. DNC-Europe also supports USAFRICOM and USCENTCOM.

EBC. An appliance that provides voice and video firewall functions. EBCs are typically located at the boundary between the edge segment and the access segment. The EBC is used to exert control over the signaling and media streams and is involved in setting up, conducting, and terminating sessions.

ELSC. An Assured Service Session Initiation Protocol (AS-SIP) signaling device in the DISN or in a DoD Component network that serves more than one LSC and that directly serves Internet Protocol (IP) end instruments (EIs).

End Device (ED). The primary user interface (e.g., smartphones, tablets, softphones, desktop phones, etc.) to customers. EDs are the user appliances that initiate, accept, and/or terminate a UC session. EDs may be standalone applications or may be used in conjunction with other applications (e.g., softphone). EDs may provide a single service (e.g., voice, video, or data) or multiple services.

End-to-end. User end device to user end device.

Internet Access Point. A network exchange facility where Internet Service Providers (ISPs) connect with the DoD networks in a peering arrangement. The connections within IAPs determine traffic routing to DoD networks and the Internet.

LSC. Assured Service Session Initiation Protocol (AS-SIP) signaling device at a base/post/camp/station that directly serves Internet Protocol (IP) end instruments (EIs).

MFS. A switch that combines the tandem function of the stand alone switch with the end-office function of connecting the users lines to the backbone trunk.

MFSS. The MFSS is an MFS that is enhanced with an Internet Protocol (IP) interface. As with any MFS, the MFSS supports End Office and Tandem Switch capabilities. In addition, the MFSS also includes LSC and Assured Real Time Services (ARTS) Softswitch (SS) functions to support line-side IP EI and trunk-side Assured Service Session Initiation Protocol (AS-SIP) and AS-SIP for Telephones signaling.

Multi-Carrier Entry Point.   A central access point for mobile enabled enclaves to a host of wireless carriers. The MCEP serves as a gateway for all data traffic to and from mobile devices for both the unclassified and classified data.

Pilots. The demonstration of UC capabilities to ensure that UC products are interoperable, secure, and compliant.

Survivable Call Processor. Function that allows routine calls to be placed when connection to the enterprise is severed.

UC. The integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities.

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

UC Operational Framework. The UC Operational Framework is intended to guide and align DoD Component instantiation of respective implementation plans and solutions. It provides a common language and reference for DoD Components' implementation of UC technology, supports implementation of DoD Component solutions, and encourages adherence to common standards and specifications.

UC Spirals. A subset of UC capabilities deployed as part of the UC Pilot.

UC transport. The secure and highly available enterprise network infrastructure used to provide voice, video, and/or data services through a combination of DoD and commercial terrestrial, wireless, and satellite communications capabilities.

WAN SS. An IP DISN backbone component that supports LSC, ELSC, and Tandem Switch capabilities. In addition, the WAN SS can include, as an option, an LSC and Softswitch (SS) functions to support line-side IP end instrument and trunk-side Assured Service Session Initiation Protocol (AS-SIP) and AS-SIP for signaling.