Department of Defense
INSTRUCTION

NUMBER 8100.04
December 9, 2010

ASD(NII)/DoD CIO

SUBJECT: DoD Unified Capabilities (UC)

References: 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 (hereafter referred to as "acquisition"); 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.,

circuit-switched and/or Internet protocol (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, during each phase of those products’ life cycles, from acquisition to operations.

(3) UC support for authorized non-DoD users (e.g., combined or coalition partners and U.S. Government departments and agencies).

(4) Acquisition of services as described in DoDD 5000.01 (Reference (f)) and DoDI 5000.02 (Reference (g)).

b. This Instruction does NOT apply to:

(1) DoD Component acquisition programs governed by References (f) and (g) and Chairman of the Joint Chiefs of Staff Instruction 3170.01G (Reference (h)), except as stated in subparagraph a.(4) of this section; however, the DoD Components are encouraged to use UC-certified products in developing acquisition programs, where appropriate.

(2) DoD cryptologic Special Compartmented Information systems and classified cryptologic products, pursuant to DoDI 8500.2 (Reference (i)).

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. The DoD Components shall integrate current network technologies with future network technologies to provide UC (i.e., any single or combination of information media (voice, video, and/or data), whether converged or non-converged) on DoD networks.

b. Products that provide or support UC, acquired or operated by the DoD Components, shall be certified for interoperability and information assurance (IA) as set forth in this Instruction.

c. The DoD Components shall comply with functional requirements, performance objectives, and technical specifications for DoD networks that support UC, as specified in Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) publication (Reference (j), commonly known and hereafter referred to as the “DoD Unified Capabilities Requirements (UCR)”).

d. DoD networks shall support UC during all phases of DoD operations.

e. The ASD(NII)/DoD CIO shall grant non-DoD activities connection to DoD networks that support UC when necessary for national security, when not in conflict with local ordinances, when those activities have critical national security and emergency preparedness needs, and when connection is in the best interest of the U.S. Government.

(1) Connection shall only be provided to non-DoD or nongovernmental activities or agencies (Federal agencies, State government organizations, DoD contractors, foreign government organizations and entities, and combined or coalition forces) on a not-to-interfere basis.

(2) All authorized non-DoD users shall comply with approved UCR interfaces.

(3) All non-DoD users shall be sponsored by a DoD Component.

f. The Defense Information Systems Agency (DISA) is the preferred UC transport provider for Internet and commercial satellite connections used for voice, video, and/or data services on DoD networks. The DoD Components shall be permitted to use non-DISA enterprise-level infrastructures only if such infrastructure adheres to the UCR and either:

(1) A compelling business case justification is provided to and approved by the ASD(NII)/DoD CIO; or

(2) The Head of the OSD or DoD Component, in coordination with the Director, DISA, provides a justification to the ASD(NII)/DoD CIO that unique mission requirements cannot be met by DISA.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

8. EFFECTIVE DATE. This Instruction is effective immediately.

Teresa M. Takai
Acting Assistant Secretary of Defense for
Networks and Information Integration/DoD
Chief Information Officer

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

TABLE

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005

(b) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009

(c) DoD Directive 4640.13, "Management of Base and Long-Haul Telecommunications Equipment and Services," December 5, 1991 (hereby cancelled)

(d) DoD Instruction 4640.14, "Base and Long-Haul Telecommunications Equipment and Services," December 6, 1991 (hereby cancelled)

(e) DoD Instruction 8100.3, "Department of Defense (DoD) Voice Networks," January 16, 2004 (hereby cancelled)

(f) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003

(g) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008

(h) Chairman of the Joint Chiefs of Staff Instruction 3170.01G, "Joint Capabilities Integration and Development System," March 1, 2009

(i) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

(j) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Publication, "Department of Defense Unified Capabilities Requirements," current edition[1]

(k) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004

(l) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004

(m) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002

(n) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007

(o) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "DoD Unified Capabilities Approved Products List," current edition[2]

(p) DoD Instruction 8410.02, "NetOps for the Global Information Grid (GIG)," December 19, 2008

(q) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition

(r) DoD Directive 5100.35, "Military Communications-Electronics Board (MCEB)," March 10, 1998

[1] Available on the Internet at http://www.disa.mil/ucco/

[2] Available on the Internet at http://www.disa.mil/ucco/

ENCLOSURE 2

RESPONSIBILITIES

1. ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO, in addition to the responsibilities in section 4 of this enclosure, shall:

a. Maintain this Instruction in coordination with the Heads of the other OSD and DoD Components.

b. Provide overall policy and direction for the development of UC requirements and approve the UCR for use in test and certification of UC products. In conjunction with the Chairman of the Joint Chiefs of Staff, develop and issue implementing instructions for the test, certification, acquisition, installation, transport, connection, and operation of DoD networks to support UC.

c. Establish policy and provide oversight for all DoD networks that support UC.

(1) Establish policy, processes, and responsibilities to ensure compliance with DoDD 4630.05 and DoDI 4630.8 (References (k) and (l)) requirements for interoperability and supportability of products that provide UC on DoD networks.

(2) Ensure compliance with Reference (i) and DoDD 8500.01E and DoDI 8510.01 (References (m) and (n)) requirements for IA certification and accreditation (C&A) of information systems (IS) supported by UC.

(3) Establish a process for adjudicating requests for waivers of DoD UC policy and requests for Interim Certificates to Operate (ICTO) as set forth in section 6 of Enclosure 3.

(4) Establish policy, processes, and responsibilities for non-DoD user access to DoD networks that support UC.

d. Approve functional requirements, performance objectives, and technical specifications for DoD networks that support UC, as specified in the UCR.

e. In consultation with the Chairman of the Joint Chiefs of Staff, approve the biennial UC Master Plan (UC MP) provided by the Director, DISA, pursuant to subparagraph 2.b.(3) of this enclosure.

f. Establish a UC governance structure that includes a DoD UC Steering Group (SG) and a DoD UC Industry Advisory Council (IAC) as set forth in section 1 of Enclosure 3.

2. DIRECTOR, DISA. The Director, DISA, under the authority, direction, and control of the ASD(NII)/DoD CIO and, in addition to the responsibilities in section 4 of this enclosure, shall:

a. Establish procedures and technical requirements for the test, certification, acquisition, installation, connection, and operation of DoD networks to support UC.

b. Designate an office responsible for UC technology insertion in support of UC that shall:

(1) Provide direction and technical guidance for DoD networks that support UC.

(2) In coordination with the DoD Components, define functional requirements, performance objectives, and technical specifications for DoD networks that support UC to be contained in the UCR and approved by ASD(NII)/DoD CIO.

(3) Provide to the ASD(NII)/DoD CIO and the Chairman of the Joint Chiefs of Staff a biennial UC MP to include DoD-wide UC migration planning and investment guidance, a UC architecture, an assessment of the ability to meet performance requirements and planned schedules, a mitigation plan for security risks, and resource requirements for meeting the UC migration strategy.

c. In coordination with the DoD Components, define DoD UC directory, addressing, and numbering schemas for approval by the appropriate ASD(NII)/DoD CIO governance board or committee.

d. Ensure products that support UC on DoD networks comply with Reference (k) and (l) requirements for interoperability and supportability, and Reference (m) and (n) requirements for IA.

e. Serve, through the DISA Joint Interoperability Test Command (JITC), as the interoperability certification authority (CA) for products that support UC on all DoD networks; and as the IA CA for products that support UC on only DISA-owned or -operated networks.

f. Establish UC product security requirements to include configuration requirements in the development of UC Security Technical Implementation Guides (STIGs) and verify compliance with UC-related STIGs during assessments or inspections.

g. Provide UC transport for the DoD Components.

h. Review DoD Component requests for UC transport, determine the most effective and economical UC transport solution set, and approve DoD Component requests, pursuant to paragraph 4.f., as appropriate.

i. Establish UC connection approval process requirements, and approve DoD Component requests to install and connect UC products to DoD networks.

j. Review all requests for waivers of UC policy and for ICTOs. Provide recommendations to the Military Communications-Electronics Board (MCEB) for consideration and forwarding to the ASD(NII)/DoD CIO for approval.

k. Develop and maintain the UCR to establish the functional requirements, performance objectives, and technical specifications for DoD networks that support UC. Use the UCR to develop test plans (TPs) for UC certification of interoperability and IA.

l. Through the DISA UC Certification Office (UCCO), develop and maintain the ASD(NII)/DoD CIO UC Approved Products List (APL) (Reference (o), hereafter referred to as the "APL") of certified products that provide UC on DoD networks.

m. Review and approve use of network interfaces not conforming to the UCR. Recommend options for controlling and monitoring the flow of traffic across the non-conforming network interfaces.

n. In conjunction with the Commander, United States Strategic Command (CDRUSSTRATCOM), support DoD Component operations and missions by maintaining situational awareness of networks that support UC, and conduct network configuration changes in accordance with DoDI 8410.02 (Reference (p)), as required by the CDRUSSTRATCOM, pursuant to paragraph 7.c. of this enclosure.

o. Coordinate with NSA and other DoD Components in the development of the UCR, UC TPs and STIGs.

p. Provide representatives to the DoD UC SG and the DoD UC IAC.

3. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS). The DIRNSA/CHCSS, under the authority, direction, and control of the Under Secretary for Intelligence and in addition to the responsibilities in section 4 of this enclosure, shall:

a. Support DISA in the development of the UCR, UC TPs, and STIGs.

b. Provide a representative to the DoD UC SG and the DoD UC IAC.

4. HEADS OF THE OSD AND DoD COMPONENTS. The Heads of the OSD and DoD Components shall:

a. Ensure their respective Components implement the requirements and policies of this Instruction.

b. Ensure their respective Components provide UC to DoD and non-DoD authorized users in accordance with:

(1) References (i), (k), and (l) requirements for interoperability and supportability, and References (m) and (n) requirements for IA. Ensure products that support UC on DoD Component-owned networks are tested pursuant to the UCR, and are UC certified for interoperability by JITC and for IA by the DoD Component designated accrediting authorities (DAAs).

(2) Reference (n) requirements for IA C&A for DoD IS that are supported by UC on DoD Component-owned networks.

(3) The UC APL for acquisition and operation of products that provide UC on DoD Component-owned networks.

(4) The DISA UC directory, addressing, and numbering schemas to ensure standardization and interoperability across DoD networks.

c. Implement functional requirements, performance objectives, and technical specifications for DoD networks that support UC, as specified in the UCR. Ensure TPs are based on the UCR and are prepared for all products that provide UC on DoD Component-owned networks.

d. Ensure their respective Component networks that support UC comply with approved UCR interfaces. Use of network interfaces not conforming to the UCR shall not be permitted without DISA technical review and approval on a site-specific basis.

e. Comply with assured service features (ASFs) requirements (assured system and network availability, assured information protection, and assured information delivery) as defined in the Glossary and amplified in the UCR.

f. Operate DoD Component-owned networks that support UC with the capability to assign resources on demand, consistent with mission priorities.

(1) For voice and video sessions, precedence-based assured service capability shall be provided to permit higher-precedence users to preempt lower-precedence sessions at the edge of the network.

(2) The network shall be rapidly reconfigurable to assign resources consistent with the situation to ensure minimal blocking to services critical to the response.

g. Submit to the Director, DISA, requests for UC transport, regardless of technology implemented, for consideration and approval, pursuant to paragraph 4.f..

h. Define and coordinate functional requirements, performance objectives, and technical specifications for DoD networks that support UC for potential inclusion in the UCR. Forward requirements to the Director, DISA, for validation and to the ASD(NII)/DoD CIO for final approval.

i. Plan, program, and budget for UC requirements guided by the UC MP.

j. Provide read-access and limited and/or controlled write-access capabilities to their respective Component-owned networks to DISA and USSTRATCOM, using DISA-defined network operations information sharing services in accordance with Reference (p), to enable situational awareness and allow for network modifications pursuant to paragraphs 2.n., 7.b., and 7.c. of this enclosure.

k. Report to the Director, DISA, any user locations where UCR performance requirements (e.g., quality of service) cannot be achieved due to resource or operational limitations.

l. Review all requests for waivers of UC policy and for ICTOs. Provide recommendations to the MCEB and the Director, DISA, for consideration and forwarding to the ASD(NII)/DoD CIO for approval.

5. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments, in addition to the responsibilities in section 4 of this enclosure, shall each provide a representative to the DoD UC SG and the DoD UC IAC.

6. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff, in addition to the responsibilities in section 4 of this enclosure, shall:

a. In conjunction with the ASD(NII)/DoD CIO, develop and issue implementing instructions for the test, certification, acquisition, transport, connection, and operation of DoD networks to support UC.

b. Validate UC joint operational functional requirements and performance objectives for inclusion in the UCR.

c. Validate the UC MP.

d. Validate and forward to the ASD(NII)/DoD CIO for approval:

(1) Requests from non-DoD agencies, organizations, activities, or entities for access to UC on DoD networks.

(2) Combatant Command requests for waivers of UC policy and for ICTO.

(3) All requests for waivers of UC policy and for ICTO that are based upon urgent operational needs.

e. Provide representatives to the DoD UC SG and the DoD UC IAC.

7. CDRUSSTRATCOM. The CDRUSSTRATCOM, in addition to the responsibilities in section 4 of this enclosure, shall:

a. Direct operations and defense of UC supported by DoD networks.

b. In conjunction with the Director, DISA, support DoD Component operations and missions by maintaining situational awareness of networks that support UC.

c. Coordinate with the Director, DISA, to direct the DoD Components to change configurations of respective DoD network infrastructures that support UC as needed to ensure network operations and defense in accordance with Reference (p).

d. Provide representatives to the DoD UC SG and the DoD UC IAC.

ENCLOSURE 3

PROCEDURES

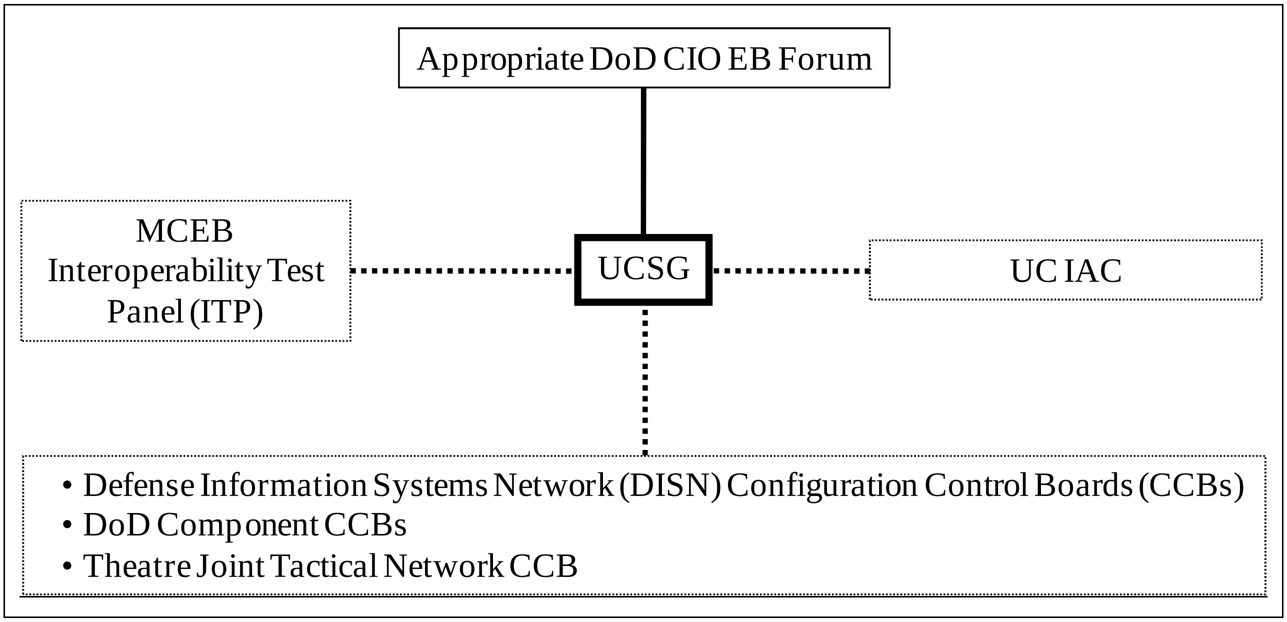
1. UC GOVERNANCE

a. General

(1) In accordance with paragraph 1.f. of Enclosure 2, the ASD(NII)/DoD CIO shall establish a UC governance structure that includes a DoD UC SG and a UC IAC. The DoD UC SG and UC IAC shall be subordinated to an appropriate DoD CIO Executive Board (EB) forum, as determined by the ASD(NII)/DoD CIO.

(2) Figure 1 depicts the UC governance structure.

Figure 1. UC Governance Structure


Appropriate DoD CIO EB Forum
MCEB Interoperability Test Panel (ITP)
UCSG
UC IAC
• Defense Information Systems Network (DISN) Configuration Control Boards (CCBs)
• DoD Component CCBs
• Theatre Joint Tactical Network CCB

b. DoD UC SG. The DoD UC SG shall:

(1) Be chaired by a designee appointed by the ASD(NII)/DoD CIO, with representatives at the O-6/GS-15 level from the Joint Staff, USSTRATCOM, the Military Departments, DISA, and NSA/CSS.

(2) Provide a forum to coordinate policy and provide oversight and direction across DoD organizations in support of DoD UC implementation. The DoD UC SG shall propose, review, and coordinate UC policies and requirements; review critical UC issues; and define associated strategies for addressing these issues.

(3) Synchronize DoD Component UC efforts across the collective areas of responsibility of its membership to ensure that policies meet DoD objectives, timeframes for implementation are coordinated, and DoD UC activities evolve to meet emerging operational and technical requirements.

(4) Interface, as required, with the MCEB; the DISN, DoD, and Theatre Joint Tactical Network CCBs; and the DoD UC IAC.

c. DoD UC IAC. The DoD UC IAC shall:

(1) Be chaired by a designee appointed by the ASD(NII)/DoD CIO, with representatives from the Joint Staff, USSTRATCOM, DISA, NSA/CSS, and UC product vendors.

(2) Foster effective collaboration between DoD UC stakeholders and UC product vendors, promote the development and certification of products, identify issues of common interest to the Department of Defense and UC vendors, and create a forum to discuss UC policy and requirements with industry.

2. UC TECHNICAL IMPLEMENTATION DOCUMENTS. DISA shall develop and maintain these UC technical documents, which shall apply to all products that provide UC:

a. UCR. The UCR shall specify the functional requirements, performance objectives, and technical specifications for DoD networks that support UC, and shall be used to support test, certification, acquisition, connection, and operation of these devices. It may also be used for UC product assessments and/or operational tests for emerging UC technology. DISA shall translate DoD Component functional requirements into engineering specifications for inclusion into the UCR, which shall identify the minimum requirements and features for UC applicable to the overall DoD community. The UCR shall also define interoperability, IA, and interface requirements among products that provide UC. The IA portion of the UC TP shall be based on the requirements of the UCR as derived from Reference (i).

b. UC MP. The UC MP shall define the migration strategy to converged, net-centric, IP-based voice, video, and/or data services. The UC MP shall serve as a guideline to the DoD Components in the preparation of migration plans and acquisition plans for phasing in voice and video over IP services and other UC that will operate in converged voice, video, and/or data networks. The UC MP provides guidance for DoD Component program objective memorandum submissions.

c. UC TP. JITC shall, in collaboration with other DoD Components, develop the UC TP and formats for reporting interoperability and IA test results. The UC TP shall specify interoperability and IA test criteria for products that provide UC. The UC TP shall address interoperability and IA requirements for the products identified in the UCR. The UC TP shall evaluate security features within the existing network and critical areas involving assured services and new UC technology. The UC TP shall also address security features between new technologies, new technologies and the existing network, and the performance impact of these new technologies on assured services. The IA portion of the UC TP shall be based on the UCR and STIGs as derived from Reference (i). The UC TP supports the test and certification process.

d. STIGs. The STIGs shall provide the technical security guidelines, requirements, and implementation details for the security features required for products that provide UC. The STIGs shall be used to support test, certification, acquisition, operation, and implementation procedures, and to assist in meeting minimum requirements, standards, controls, and options for protecting network operations. IA testing shall be conducted pursuant to applicable STIGs, prior to operation of products that provide UC.

3. UC TRANSPORT REQUESTS

a. The DoD Components shall submit to DISA all requests for UC transport, regardless of technology used, for consideration and approval, pursuant to paragraph 4.f..

b. DISA shall review all DoD Component requests for UC transport, determine the most cost effective UC transport solution set, and approve DoD Component requests, pursuant to paragraph 4.f., as appropriate.

c. If a DoD Component desires an exemption to the DISA recommended solution set, the DoD Component shall forward a waiver request through the chain of command in accordance with paragraph 6.b. of this enclosure. The Chairman of the Joint Chiefs of Staff shall validate UC transport requests only when an urgent operational need exists. The Director, DISA, shall analyze the waiver request, provide a technical impact assessment, and forward the request to the ASD(NII)/DoD CIO for consideration, adjudication, and approval.

d. Waivers shall be reviewed annually by the Director, DISA, and the ASD(NII)/DoD CIO to determine if the waiver should remain in effect.

4. UC CERTIFICATION FOR INTEROPERABILITY AND IA, AND CONNECTION APPROVAL, PROCESSES

UC products acquired by the DoD Components, and connected or planned for connection to DoD networks, shall be both interoperability and IA certified pursuant to the UCR or an approved information support plan that includes UC products.

a. UC Certification for Interoperability and Connection Approval Processes. All UC products shall be tested and certified for interoperability.

(1) The ASD(NII)/DoD CIO shall provide overall policy and direction for development of UC requirements. DISA shall translate DoD Component functional requirements into engineering specifications for inclusion into the UCR. The ASD(NII)/DoD CIO shall approve the UCR for use in test and certification of UC products. JITC shall develop the UC TP based on the UCR. The UCR may also be used for UC product assessments and/or operational tests for emerging UC technology.

(2) JITC shall conduct interoperability testing, adjudicate interoperability test results with all parties concerned, and provide certification as appropriate. Figure 2 depicts an overview of the UC requirements, UC certification for interoperability, and connection approval processes. JITC shall employ distributed testing for UC certification for interoperability as set forth in section 5 of this enclosure, and shall serve as the UC interoperability certifying authority.

(3) The UCCO shall place UC products certified for both interoperability and IA on the UC APL. The UC APL is the single authoritative source for certified UC products intended for use on DoD networks. The DoD Components are required to acquire or operate only UC products listed on the UC APL, unless, and until, a waiver is approved. The DoD Components shall issue a new or update an existing accreditation decision when UC products are installed, pursuant to Reference (n). This new or updated accreditation decision may result in an authorization to operate (ATO), interim authorization to operate (IATO), or interim authorization to test (IATT). DISA shall provide connection approval to the DISN (i.e., approval to connect (ATC) or interim approval to connect (IATC)). When installed and connected, UC products shall be operated and maintained pursuant to DISA STIGs and the JITC interoperability certified configuration.

b. UC Certification for IA and Connection Approval Processes. UC products on the UC APL shall be granted UC certification for IA by the DISA CA or the DoD Component DAA, as appropriate. DISA shall oversee the UC product certification process for IA. The DoD Component DAAs shall review UC certification determinations and issue accreditation decisions for IS employing UC products pursuant to Reference (n).

(1) DISA and other DoD Component test labs shall conduct IA testing and adjudicate IA test results for security features of products that provide UC. The DISA CA or the DoD Component DAA shall issue a UC certification for IA. Once a product has received UC certifications for both interoperability and IA, that product shall be placed on the UC APL. Figure 3 depicts the UC certification for IA and connection approval processes.

(2) IS using UC products shall be certified and accredited on a site-specific basis, as appropriate, by the DoD Component DAA as part of the overall DoD Information Assurance Certification and Accreditation Process (DIACAP) in accordance with Reference (n).

(3) As an artifact of the UC test and certification process for IA, the DoD Component test labs shall produce a UC Product DIACAP Score Card of technical IA controls tested (as DoD Component test labs will test only a sub-set of IA controls) that will be integrated into the DIACAP scorecard of ISs using the UC products. The remaining IA controls shall be tested on a site-specific basis, as appropriate, by the DoD Component owner employing the UC products, to support an enterprise-wide or DoD Component IA certification determination and accreditation decision. The UC Product DIACAP Score Card supports the IS certification and accreditation decision, and can assist a site in creating and implementing a security baseline for the UC product that supports an accreditation decision. DISA shall maintain a repository of UC Product DIACAP Score Cards for reuse by the DoD Components.

Figure 2. UC Requirements, Certification for Interoperability, and Connection Approval Processes

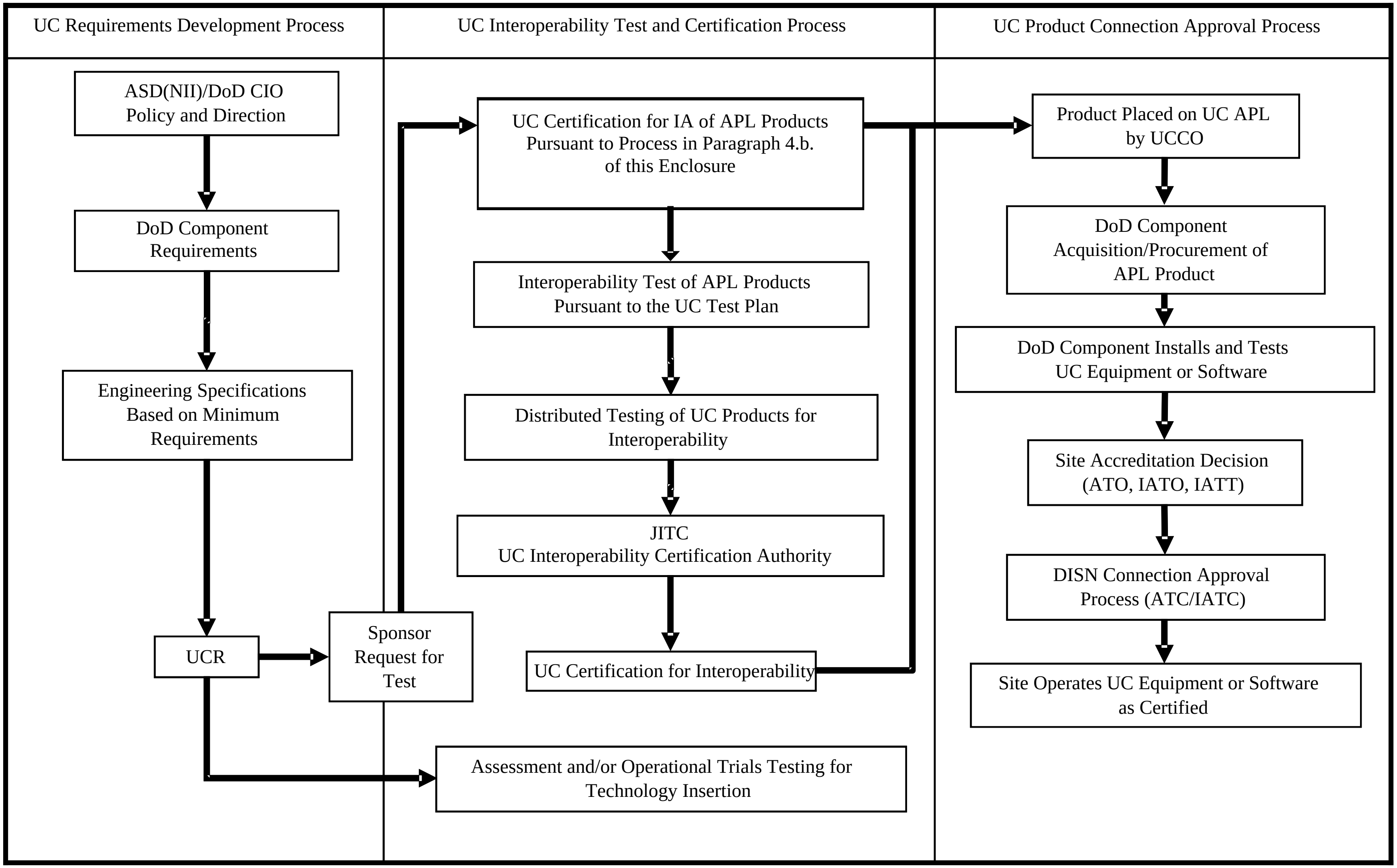
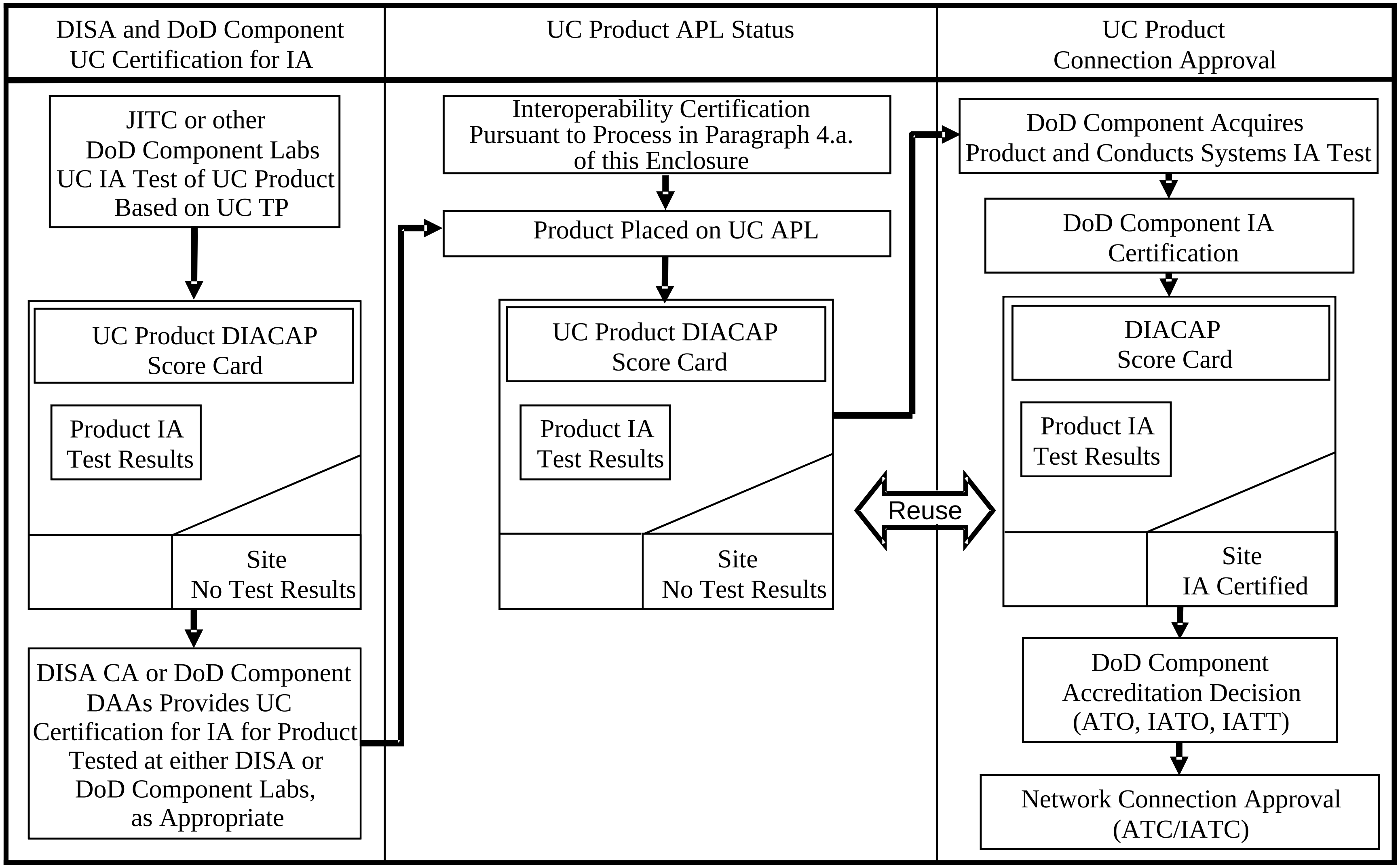

UC Requirements Development Process
UC Interoperability Test and Certification Process
UC Product Connection Approval Process
ASD(NII)/DoD CIO Policy and Direction
DoD Component Requirements
Engineering Specifications Based on Minimum Requirements
UCR
Sponsor Request for Test
UC Certification for IA of APL Products Pursuant to Process in Paragraph 4.b. of this Enclosure
Interoperability Test of APL Products Pursuant to the UC Test Plan
Distributed Testing of UC Products for Interoperability
JITC
UC Interoperability Certification Authority
UC Certification for Interoperability
Assessment and/or Operational Trials Testing for Technology Insertion
Product Placed on UC APL by UCCO
DoD Component Acquisition/Procurement of APL Product
DoD Component Installs and Tests UC Equipment or Software
Site Accreditation Decision (ATO, IATO, IATT)
DISN Connection Approval Process (ATC/IATC)
Site Operates UC Equipment or Software as Certified

Figure 3. UC Certification for IA and Connection Approval Processes


DISA and DoD Component UC Certification for IA
UC Product APL Status
UC Product Connection Approval
JITC or other DoD Component Labs UC IA Test of UC Product Based on UC TP
UC Product DIACAP Score Card
Product IA Test Results
Site No Test Results
DISA CA or DoD Component DAAs Provides UC Certification for IA for Product Tested at either DISA or DoD Component Labs, as Appropriate
Interoperability Certification Pursuant to Process in Paragraph 4.a. of this Enclosure
Product Placed on UC APL
UC Product DIACAP Score Card
Product IA Test Results
Site No Test Results
Reuse
DoD Component Acquires Product and Conducts Systems IA Test
DoD Component IA Certification
DIACAP Score Card
Product IA Test Results
Site IA Certified
DoD Component Accreditation Decision (ATO, IATO, IATT)
Network Connection Approval (ATC/IATC)

5. UC DISTRIBUTED TEST CONCEPT

a. DISA shall employ a distributed test capability that includes test and certification of voice, video, and/or data products to accommodate the expanded scope of the UCR, and to keep pace with emerging technology and the large demand from the DoD Components for interoperable and secure products. These demands and technology challenges require the Department of Defense to incorporate DoD Component test labs in the test and certification processes. The precepts of the distributed test program are to "test once for many," create a single UC APL for use by the DoD Components in acquisitions and procurements, and more effectively integrate industry into the test and certification process. Additionally, distributed testing will facilitate more timely delivery of emerging UC technologies to the warfighter.

b. Only product categories approved by the UCSG for inclusion in the UCR shall be tested and certified for inclusion on the UC APL. The level of testing required shall be guided by the UC Test Requirements Table. The Director, DISA, in coordination with the ASD(NII)/DoD CIO shall resolve issues in interpretation and use of this table.

c. The objective of distributed testing is to leverage existing DoD Component test and evaluation capabilities and activities that already support DoD testing of products that support UC. Under this concept:

(1) JITC and other DISA labs shall serve as the primary test labs for UC products that support DISA-operated UC, and shall collaborate with other DoD Component labs for testing of emerging UC technologies.

(2) The DoD Component labs shall be the primary test labs for UC products that are acquired and deployed at the bases, camps, posts, or stations of the Component concerned.

(3) The DoD Components shall provide the results of UC testing to JITC for UC certification of interoperability, in a JITC-prescribed format. DISA shall oversee the UC testing and certification process for IA conducted by the DoD Components. JITC and all other approved DISA testing labs shall provide the results of UC IA testing to the DISA CA. The approved DoD Component testing labs shall provide the results of the UC IA testing to the sponsoring DoD Component DAA for IA certification.

(4) There shall be a single UC APL for use by the DoD Components for acquisition of UC products.

(5) A DoD Component shall sponsor each vendor product. Vendor and commercial off-the-shelf products shall only be tested once (i.e., by one DoD Component) to gain UC APL status. The DoD Component sponsors or vendors shall reimburse the respective Component labs for costs associated with UC tests conducted.

(6) The Defense IA Security Accreditation Working Group established in Reference (n) shall serve as the advisory panel to the DISA CA for resolution of enterprise-wide IA issues that cannot be independently resolved during DoD Component IA testing.

Table. UC Test Requirements

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

(7) UC products shall be recertified for interoperability and IA every 3 years, or when significant software upgrades are made that impact either interoperability or IA.

(8) The UCCO shall manage the UC distributed test and certification processes to include schedule coordination, vendor orientation, test status monitoring, results posting, UC APL maintenance, and UC test requirements and results adjudication.

6. <u>REQUESTS FOR WAIVERS OF DoD UC POLICY AND ICTOs</u>

a. Only the ASD(NII)/DoD CIO is authorized to approve requests for waivers of DoD UC policy and requests for ICTOs.

(1) The ASD(NII)/DoD CIO shall grant waivers to DoD UC policy only:

(a) When the operational chain of command and the Chairman of the Joint Chiefs of Staff have validated an urgent operational need, or;

(b) To accommodate the introduction of new or emerging technology pilot programs that have been coordinated with and recommended by the Director, DISA, and validated by the Head of the OSD or DoD Component concerned.

(2) The ASD(NII)/DoD CIO shall grant ICTOs only when:

(a) The operational chain of command and the Chairman of the Joint Chiefs of Staff have validated an urgent operational need requiring UC product fielding prior to testing;

(b) JITC and other DoD Component labs are unable to assess all required interfaces for the UC products undergoing testing, or;

(c) DISA has completed a satisfactory technical assessment of interface criteria for non-DoD user installations.

b. To obtain a waiver to UC policy or to request an ICTO, the acquiring activity shall:

(1) Prepare a site-specific request, to include: for waivers, the reason compliance is not possible; for ICTOs, the reason the product must be fielded before testing; and for both, the proposed equipment configuration.

(2) Forward the request through the chain of command, then through the Chairman of the Joint Chiefs of Staff to the ASD(NII)/DoD CIO or, for interoperability-related requests, to the MCEB, for consideration and adjudication. For interoperability-related requests, the sponsor shall forward the request to the Director, DISA, first; then the Director, DISA, shall provide a recommendation to the MCEB and the ASD(NII)/DoD CIO for disposition of the waiver or ICTO request. The MCEB may deny the acquiring activity’s request, or may forward a recommendation for approval to the ASD(NII)/DoD CIO for decision.

c. Waivers to UC policy and ICTOs shall not be granted for a period of more than 1 year. Only in exceptional circumstances, and with ASD(NII)/DoD CIO approval, shall extensions of waivers or ICTOs be granted. DISA shall maintain a database to track the status of granted waivers and ICTOs.

d. When an ICTO has been granted, the acquiring activity shall update the MCEB on certification progress as required. DISA shall consider for disconnection from the network UC products that are not interoperability certified within the specified period of the waiver or ICTO.

7. REQUESTS FOR WAIVERS OF IA POLICY. Waivers of DoD IA policy and requirements shall not be granted under the provisions of this Instruction.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

APL	Approved Products List
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
ASF	assured service feature
ATO	authorization to operate
C&A	certification and accreditation
CA	Certification Authority
CCB	Configuration Control Board
DAA	Designated Accrediting Authority
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoDD	DoD Directive
DoDI	DoD Instruction
EB	executive board
IA	information assurance
IAC	Industry Advisory Council
IATC	interim approval to connect
IATO	interim authorization to operate
IATT	interim authorization to test
ICTO	interim certificate to operate
IP	Internet protocol
IS	information system(s)
ITP	Interoperability Test Panel (MCEB)
JITC	Joint Interoperability Test Command (DISA)
MCEB	Military Communications-Electronics Board
MP	master plan
NSA/CSS	National Security Agency/Central Security Service
SG	steering group
STIG	Security Technical Implementation Guide
TP	test plan

UC	Unified Capabilities
UCCO	Unified Capabilities Certification Office (DISA)
UCR	Unified Capabilities Requirements

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

accreditation decision. Defined in Reference (i).

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.

ATO. Defined in Reference (n).

authorized user. Any appropriately approved DoD or non-DoD individual or organization with a requirement to access DoD UC for performing or assisting in a lawful and authorized government function.

CA. Defined in Reference (n).

certification determination. Defined in Reference (i).

connection approval. Defined in Reference (i).

DAA. Defined in Reference (n).

DIACAP. Defined in Reference (n).

DIACAP Score Card. Defined in Reference (n).

IA accreditation decision. Defined in Reference (n).

IA certification. Defined in Reference (n).

IA control. Defined in Reference (i).

IATO. Defined in Reference (n).

IA. Defined in Joint Publication 1-02 (Reference (q)).

MCEB. A decision-making body chaired by the Joint Staff Director for Command, Control, Communications, and Computer Systems and composed of the command, control, communications, computers, and intelligence principals of the Military Services and the Directors of DISA, the Defense Intelligence Agency, and the National Security Agency. This body deals with issues of interoperability and standardization of communications and computer systems between the Department of Defense and U.S. allies. (See DoDD 5100.35 (Reference (r)).)

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 Product DIACAP Score Card. A summary report that provides the implementation status of IA controls for UC products tested.

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.