# DoD INSTRUCTION 8330.01

# INTEROPERABILITY OF INFORMATION TECHNOLOGY, INCLUDING NATIONAL SECURITY SYSTEMS

| | |
|---|---|
| **Originating Component:** | Office of the DoD Chief Information Officer |
| **Effective:** | September 27, 2022 |
| **Releasability:** | Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/. |
| **Reissues and Cancels:** | DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014, as amended |
| **Approved by:** | John B. Sherman, DoD Chief Information Officer |

**Purpose:** In accordance with the authority in DoD Directive (DoDD) 5144.02 and the guidance in DoDD 8000.01, this issuance:

- Establishes policy, assigns responsibilities, and provides direction for certifying the interoperability of information technology (IT) and national security systems (NSS) pursuant to Sections 2222, 2223, and 2224 of Title 10, United States Code.
- Establishes a capability-focused, architecture-based approach for interoperability analysis.
- Establishes the Interoperability Steering Group (ISG).
- Establishes the governing policy and responsibilities for interoperability requirements development, test, certification, and prerequisites for connection of IT, including NSS.
- Requires DoD IT and NSS, and embedded systems and subsystems to plan, resource, and verify interoperability for all data exchanges internal and external to the overarching system or platform.
- Defines a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) approach to enhance life-cycle interoperability of IT.

# TABLE OF CONTENTS

# SECTION 1: GENERAL ISSUANCE INFORMATION

## 1.1. APPLICABILITY.

a. This issuance applies to:

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

(2) The U.S. Coast Guard. The U.S. Coast Guard will adhere to DoD requirements, standards, and policies in this issuance in accordance with the January 19, 2017 Memorandum of Agreement between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations.

(3) IT, which includes any systems, applications, products and IT services, and NSS that MILDEPs, CCMDs, DAFAs, OSD Components, and their subordinate commands acquire, procure, develop, or operate that meet at least one of the following criteria:

(a) Provides direct support of DoD missions. This includes IT in development and in operation as well as certain aspects of embedded IT (e.g., in platforms that exchange information beyond the platform boundaries).

(b) Shares, exchanges, or uses data, information, and services to enable units or forces to operate in joint operations.

(c) Supports any DoD warfighting mission areas.

(d) Supports DoD mobility initiatives to include infrastructure, services, and management.

b. This issuance **does not** apply to IT that is:

(1) Only used for simulation, training, test, or experimentation.

(2) Only stores, processes, or exchanges simulated (i.e., not real-world) data.

(3) Has no capability for exporting data to an operational system.

(4) Used exclusively for demonstration or simulation. IT that imports but does not export real-world data.

(5) Does not use that data to support any operational process (e.g., warfighting, business, intelligence, enterprise information environment) or decision-making.

(6) Designated as DoD end user enterprise services and governed in accordance with DoD Instruction (DoDI) 8100.04. End user enterprise services include enterprise collaboration and productivity services (formerly unified capabilities and integrated services) and warning and safety functions supporting emergency notification and services.

## 1.2. POLICY.

a. IT that MILDEPs, CCMDs, and DAFAs develop, manage, and operate must be interoperable, to the maximum extent practical, with existing and planned systems (including applications) and equipment of joint, combined, and coalition forces, other U.S. Government departments and agencies, and non-governmental organizations, as required based on operational context.

b. To maximize interoperability, IT will, to the maximum extent practical, support, provide, and use open-source, non-proprietary, and industry standard interfaces, data, and services.

c. Programs acquiring IT and IT capabilities, including defense acquisition and procurement programs, must provide the net-ready content in the requirements documentation. The net-ready content consists of the net-ready requirements, as outlined in the Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS), also known and referred to in this issuance as the "JCIDS Manual," and the associated architecture viewpoints. These artifacts are used to assess the technical exchange of information, data, and services, and the end-to-end operational effectiveness of those exchanges through test and evaluation (e.g., developmental test and evaluation (DT&E) and operational test and evaluation (OT&E)).

d. IT interoperability must be evaluated early, in an operationally relevant environment, and with sufficient frequency throughout a system's life-cycle to capture and assess changes affecting interoperability. Interoperability testing must be comprehensive and cost effective. Before fielding a new IT capability or upgrading existing IT, complete interoperability testing, and obtain the interoperability certification.

e. IT must be certified for joint interoperability or possess an interim certificate to operate (ICTO), possess a waiver to policy, or be exempt from joint interoperability certification (e.g., joint urgent operational need) in accordance with this issuance before connecting to any operational DoD network. IT programs that fail to meet these criteria may be considered for placement on the operating at risk list (OARL). In addition, IT must possess a valid authorization to operate or interim authorization to test, in accordance with DoDI 8510.01, before connection to any DoD network.

f. IT developers and operators must fully comply with the cybersecurity requirements of DoDIs 8500.01 and 8510.01.

g. Execution of the guidance in this issuance must be tailored, in coordination with the ISG, to comply with Director of National Intelligence (DNI) directives, Intelligence Community (IC) policies, and DoD intelligence policies. Special measures may be required for the protection and handling of information including, but not limited to, foreign intelligence, counterintelligence (CI) information, controlled unclassified information, and U.S. person information.

h. This issuance does not alter or supersede existing authorities and policies of the DNI regarding the protection of sensitive compartmented information and special access programs pursuant to Executive Orders 12333 and 13526, national security information systems pursuant to Executive Order 13231, and other laws and regulations.

# SECTION 2: RESPONSIBILITIES

## 2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO).

In addition to the responsibilities in Paragraph 2.13., the DoD CIO:

a. Maintains this issuance in coordination with the other OSD Component heads, the Secretaries of the MILDEPs, CJCS, Combatant Commanders (CCDRs), and Directors of the DAFAs.

b. Provides oversight of IT interoperability, in coordination with the other OSD Component heads, the Secretaries of the MILDEPs, CJCS, CCDRs, Directors of the DAFAs, and DoD Component organizations.

c. Establishes policy and guidance, and provides oversight for:

(1) Developing a capability-focused, architecture-based approach to achieve IT interoperability.

(2) Interoperability testing, certification, connection, and operation of IT.

(3) Requesting ICTOs for IT with joint or interoperability requirements or adjudicating requests for waivers in accordance with this issuance.

(4) Achieving interoperability of data, information, and IT services.

(5) The OARL.

d. Maintains the DoD Information Enterprise Architecture (DoD IEA) pursuant to Section 1425 of Title 40, United States Code.

e. Requires that IT architecture, such as enterprise, reference, and solution information, is sufficient to assess interoperability.

f. Coordinates with the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), the Under Secretary of Defense for Research and Engineering (USD(R&E)), the Director of Operational Test and Evaluation (DOT&E), CJCS, the Secretaries of the MILDEPs, the CCDRs, the Directors of the DAFAs, and other OSD Component heads, to assign responsibilities and prescribe procedures to require appropriate interoperability assessment and reassessment throughout a system's life-cycle.

g. Coordinates with Secretaries of the MILDEPs, CJCS, CCDRS, and Directors of the DAFAs, to oversee the establishment of measurable and testable certification criteria for interoperability assessments.

h. Coordinates with Under Secretary of Defense for Intelligence and Security (USD(I&S)) to maintain liaison with the IC Chief Information Officer (CIO) within the Office of the DNI to identify and resolve DoD and IC interoperability issues.

i. Designates the DoD Information Technology Portfolio Repository (DITPR) and the associated SECRET Internet Protocol Router Network (SIPRNET) IT Registry as the authoritative inventories of IT systems pursuant to Section 2223(a)(5) of Title 10, United States Code.

j. Establishes the ISG, subordinate to the appropriate forum as determined by the DoD CIO.

k. Designates an ISG Tri-Chair, along with USD(A&S), and CJCS representatives, to resolve interoperability issues.

l. Publishes and maintains the ISG charter in accordance with this issuance.

m. Establishes and oversees the DoD-wide process for the review of information support plans (ISPs).

(1) Coordinates with USD(A&S), USD(R&E), DOT&E, CJCS, and USD(I&S).

(2) Develops processes, procedures, format, and content guidance for submitting ISPs.

(3) Coordinates with the Secretaries of the MILDEPs, CJCS, CCDRs, and Directors of the DAFAs in establishing ISP review processes to support joint reviews of their systems.

(4) Adjudicates critical comments in joint ISP reviews that cannot be resolved at the Secretaries of the MILDEPs, CJCS, CCDRs, and DAFAs Director level.

(5) Designates certain ISPs affecting DoD enterprise strategic initiatives for DoD special interest oversight, and participates in the ISP reviews of those systems.

(6) Assess ISPs for compliance with DoD CIO architecture, cybersecurity, spectrum, and standard policies in support of the joint reviews.

n. Establishes and oversees the DoD-wide process for achieving a joint interoperability certification of IT and NSS.

o. Addresses specific recommendations for critical IT interoperability issues within the DoD CIO Annual Defense Planning Guidance to the Secretaries of the MILDEPs, CJCS, CCDRs, Directors of the DAFAs, and OSD Component heads that support the future Planning, Programming, Budgeting, and Execution cycle.

p. Confirms Subtitle III of Title 40, United States Code, also known and referred to in this issuance as the "Clinger-Cohen Act of 1996," compliance for joint systems and delegates Clinger-Cohen Act of 1996 compliance authority for all other systems to the DoD Components CIOs.

## 2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA).

Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in Paragraph 2.13., the Director, DISA:

a. Conducts the joint IT interoperability assessment, test, and evaluation, in coordination with the Secretaries of the MILDEPs, CJCS, CCDRs, Directors of the other DAFAs, and OSD Component heads.

b. Operates and maintains the Global Information Grid Technical Guidance Federation (GTG-F) and associated processes supporting the preparation, submission, verification, assessment review, and approval of interoperability requirements (e.g., ISPs).

c. Participates in all joint reviews of joint interoperability requirements and nominates, for the DoD CIO, special interest oversight of programs with joint interoperability requirements affecting DoD enterprise strategic initiatives.

d. Provides guidance for addressing interoperability in systems engineering, planning, and program guidance, in coordination with the USD(A&S) and the USD(R&E).

e. Aids the MILDEPs, CJCS, CCMDs, other DAFAs, and OSD Components with planning early developmental IT interoperability testing to deliver solutions, reduce duplication of effort, and enhance IT interoperability.

f. Maintains the OARL, on behalf of the ISG, listing all IT systems operating on a DoD network without a joint interoperability certification, ICTO, or approved waiver to this issuance.

g. Defines the guidance for the interoperability test and certification of joint IT and NSS within DoD.

h. Uses the Defense Information Systems Network certification approval process to enforce the requirement for interoperability certification, an ICTO, or a waiver to policy in accordance with this issuance and before connection to the Defense Information Systems Network.

i. Establishes a standard approach for evaluation of critical exchange points between IT capabilities, infrastructures, and environments using measures (e.g., performance and effectiveness). Confirms interoperability from end-to-end in a multi-vendor, multi-networked, multi-service, and multinational environment, as applicable.

j. Ensures joint interoperability test criteria and joint interoperability assessment procedures address IT that supports joint cyberspace operations.

k. Coordinates with the Director, National Geospatial-Intelligence Agency (NGA), on all geospatial intelligence (GEOINT)-related joint interoperability certifications.

l. Designates a representative to serve as an ISG member.

m. Directs the Commander, DISA Joint Interoperability Test Command (JITC), to:

(1) Serve as the joint interoperability certification authority for all DoD IT with joint interoperability requirements, as described in Section 3.

(2) Serve as the ISG Executive Secretary.

(3) Coordinate with the Secretaries of the MILDEPs, CJCS, CCDRs, Directors of the other DAFAs, and OSD Component heads to establish procedures to verify, assess, and certify, through testing, joint IT interoperability throughout a system's life-cycle.

(4) Publish and maintain the Interoperability Process Guide (IPG) outlining all procedures required to support joint interoperability test, evaluation and certification, ICTO requests, waiver submissions, and OARL process.

(5) Review and provide recommendations on requests for waiver of interoperability policy in accordance with this issuance.

(6) Coordinate with the Secretaries of the MILDEPs, CJCS, CCDRs, Directors of the other DAFAs, and OSD Component heads to resolve joint IT interoperability issues. If resolution cannot be achieved, provide an impact statement and recommendations for resolution at the ISG.

(7) Participate in the joint interoperability requirements review to verify the content of the net-ready performance attribute supports joint interoperability test, evaluation, and certification in accordance with the IPG.

(8) Coordinate with program managers (PMs) of IT with joint interoperability requirements and review test and evaluation master plans (TEMPs), or equivalent, and associated developmental and operational test plans for data collection opportunities to support joint interoperability evaluation.

(9) Assess compliance with bilateral and multilateral standardization agreements (e.g., U.S.-ratified North Atlantic Treaty Organization Standardization Agreements).

(10) Provide the following, as appropriate, in support of test and evaluation activities used by the acquisition pathways (e.g., developmental testing, demonstration), for all DoD IT with joint or interoperability requirements:

(a) Status of IT interoperability and standards conformance issues.

(b) Confirmation that all required developmental testing relating to IT interoperability was successfully completed and passed.

(c) Details of any interoperability issues that must be resolved before the start of OT&E.

(11) Define the methodology to test and certify IT capabilities for interoperability within the DoD as appropriate for the IT acquisition pathway.

(12) Designate representatives to take part in applicable working groups, decision boards, or integrated process teams involved in setting or defining interoperability criteria that any IT capabilities must meet before fielding.

(13) Maintain and operate a secure test infrastructure capable of supporting interoperability test and evaluation of DISA-managed programs and programs with joint or interoperability requirements.

(14) Maintain and operate the test infrastructure consistent with the architectures and processes developed by the Test Resource Management Center (TRMC) in accordance with this issuance.

## 2.3. USD(A&S).

In addition to the responsibilities in Paragraph 2.13., USD(A&S):

a. Incorporates the policies and requirements in this issuance into the DoD documents governing acquisition (including DoDD 5000.01 and DoDI 5000.02 and its associated functional policies), and adequately addresses this guidance during IT acquisitions, as the DoD Acquisition Executive, under the authority vested in the Secretary of Defense pursuant to Sections 113 and 133b of Title 10, United States Code.

b. Approves tradeoffs among operational effectiveness, operational suitability, and interoperability, for all acquisition on oversight and procurement matters pertaining to IT acquisitions, in coordination with the DOT&E, USD(R&E), the DoD CIO, and CJCS.

c. Oversees all elements of the DoD relating to acquisition and sustainment and aid CJCS, the Secretaries of the MILDEPs, CCDRs, Directors of the DAFAs, and OSD Component heads in the evaluation of interoperability requirements in both a technical and an operational context.

d. In coordination with the DoD Business, Warfighting, Intelligence, and Enterprise Information Environment Warfighting Mission Area Owners (e.g., CJCS, USD(I&S), and DoD CIO), the Secretaries of the MILDEPs, CCDRs, Directors of the DAFAs, and OSD Component heads, requires that operationally prioritized materiel and non-materiel interoperability requirements are phased for acquisition and fielding.

e. Designates a representative to serve as an ISG Tri-Chair and to help resolve interoperability issues.

f. Assesses and considers interoperability in the Defense Acquisition Board reviews.

## 2.4. USD(R&E).

In addition to the responsibilities in Paragraph 2.13., the USD(R&E):

a. Coordinates with DoD CIO and CJCS in validating IT interoperability requirements, as described in the program's requirement documents (e.g., systems engineering plan, TEMP, ISP, capability implementation plan (CIP), capability needs statement (CNS)), are measurable, testable, and achievable during the acquisition process.

b. Establishes policy and procedures to require acquisition programs to plan and provide timely, adequate, and executable interoperability DT&E to achieve joint interoperability certification.

c. Emphasizes evaluation of IT interoperability as soon as possible during a system's development.

d. Designates a representative to serve as an ISG member.

e. Participates in joint ISP reviews as required.

f. Directs the TRMC to:

(1) Establish the architecture for a DoD enterprise-wide interoperability test capability, which must include a secure, operationally representative joint test environment.

(2) Require and verify that the MILDEPs, CCMDs, DAFAs, and OSD Components investment for test capabilities improve the overarching test capability base and provide solutions to test and evaluation shortfalls.

(3) Coordinate with the responsible MILDEPs, CCMDs, DAFAs, and OSD Components on a mutually satisfactory set of corrective actions before investments may proceed for investments determined not to be consistent with TRMC guidelines in DoDD 5105.71.

## 2.5. USD(I&S).

In addition to the responsibilities in Paragraph 2.13., the USD(I&S):

a. Advises and assists USD(A&S), DoD CIO, the Director of Cost Assessment and Program Evaluation (DCAPE), CJCS, and the Defense Acquisition Board concerning acquisition programs that affect intelligence, CI, and security capabilities and programs.

b. Serves as DoD focal point for intelligence information systems interoperability and governance processes. Coordinates, oversees, and assesses efforts of the MILDEPs, CCMDs, DAFAs, and other OSD Components to plan, program, and develop capabilities in support of intelligence information sharing, architectures, and interoperability requirements.

c. Exercises acquisition authority, as delegated by USD(A&S), DNI, or other appropriate officials, for intelligence, CI, and security technologies, systems, and equipment.

d. In coordination with CJCS and DNI, oversees the development and execution of military intelligence and national intelligence capabilities to support the CCDRs, DoD policy, and the

planning and conduct of military operations. This includes governance and oversight for the defense intelligence agencies (e.g., Defense Intelligence Agency (DIA), NGA, National Security Agency/Central Security Service (NSA/CSS), Defense Counterintelligence and Security Agency, and National Reconnaissance Office).

e. In accordance with DoD acquisition regulations, oversees research, development, test, and evaluation, in conjunction with the USD(R&E), the DOT&E, the Secretaries of the MILDEPs, CCDRs, Directors of the DAFAs, and other OSD Component heads, as appropriate.

f. Designates a representative to serve as an ISG special advisor.

## 2.6. DIRECTOR, DIA.

Under the authority, direction, and control of the USD(I&S), and in coordination with DoD CIO, in addition to the responsibilities in Paragraph 2.13., the Director, DIA:

a. In coordination with the Secretaries of the MILDEPs, CCDRs, Directors of the other DAFAs, and OSD Component heads:

(1) As appropriate, improves IT interoperability and identifies required interfaces between DIA IT and MILDEPs, CCMDs, DAFAs, and OSD Component systems.

(2) Satisfies IT interoperability requirements for processing intelligence and CI information.

(3) Resolves IT interoperability issues. If resolution cannot be achieved, provides an impact statement and recommendations for resolution to the ISG.

b. Coordinates with DoD CIO on matters involving the IT joint interoperability certification processes.

c. Designates a representative to serve as an ISG member.

## 2.7. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS).

Under the authority, direction, and control of the USD(I&S); the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor organization, of the National Security Agency, funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 2.13., the DIRNSA/CHCSS, in coordination with the DoD Chief Information Security Officer:

a. Serves as the DoD lead for signals intelligence (SIGINT) architecture and standards, in coordination with the Secretaries of the MILDEPs, CCDRs, Directors of the other DAFAs, and OSD Component heads.

b. Confirms the integration of SIGINT architecture and standards in DoD SIGINT related systems.

c. Provides cryptologic expertise and assistance in assessing IT requirements documentation for interoperability.

d. Requires interoperability and security of NSA/CSS IT with those systems that provide direct support to the CCDRs.

e. Coordinates with the Secretaries of the MILDEPs, CCDRs, Directors of the other DAFAs, and OSD Component heads to satisfy NSA/CSS-required capabilities through the design and development of interoperable IT interfaces between joint, combined, coalition, or other U.S. Government or agency IT.

f. Coordinates with the Secretaries of the MILDEPs, CCDRs, Directors of the other DAFAs, and OSD Component heads; the IC; or other U.S. Government agencies to satisfy NSA/CSS IT interoperability requirements for processing foreign intelligence and foreign CI information by designing and developing interoperable and supportable technical, procedural, and operational interfaces.

g. Coordinates with the Secretaries of the MILDEPs, CCDRs, Directors of the other DAFAs, and OSD Component heads to resolve IT interoperability issues. If resolution cannot be achieved, provide an impact statement and recommendations for resolution to the ISG.

h. Manages the interoperability requirements for cybersecurity-enabled IT products for NSS in accordance with Committee on NSS Policy No. 15.

i. Designates a representative to serve as an ISG member.

## 2.8. DIRECTOR, NGA.

Under the authority, direction, and control of the USD(I&S), in addition to their responsibilities in Paragraph 2.13., and in coordination with DoD CIO, the Director, NGA, in their capacity as the DoD GEOINT Manager:

a. Serves as the DoD lead for GEOINT.

(1) Confirms the integration of GEOINT architecture and standards in DoD GEOINT and GEOINT related systems.

(2) Provides GEOINT expertise and assistance in assessing IT requirements documentation for interoperability.

(3) Coordinates with joint interoperability certification authorities to ensure that GEOINT-related interoperability test and evaluation criteria, measures, and requirements are fulfilled before those authorities grant joint interoperability certifications.

(4) Coordinates with PMs to review IT test strategies and developmental and operational test plans to verify that all GEOINT-related requirements are addressed.

(5) Coordinates with PMs to review test results to verify that all GEOINT-related requirements are satisfied.

b. Facilitates sharing of GEOINT by the most efficient and expeditious means, consistent with DoDI 8320.02.

c. Coordinates with the Secretaries of the MILDEPs, CCDRs, Directors of the other DAFAs, and OSD Component heads to resolve IT interoperability issues. If resolution cannot be achieved, provides an impact statement and recommendations for resolution to the ISG.

d. Designates a representative to serve as an ISG member.

## 2.9. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE.

In addition to the responsibilities in Paragraph 2.13., in coordination with the Secretaries of the MILDEPs, CCDRs, Directors of the DAFAs, and other OSD Component heads, the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense:

a. Addresses IT interoperability resource issues resulting from the requirements of this issuance in the budgetary process.

b. Provides the Deputy Secretary of Defense with budget recommendations for addressing critical IT interoperability issues identified through the interoperability governance process.

## 2.10. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY.

Under the authority, direction, and control of the Under Secretary of Defense for Policy, the Assistant Secretary of Defense for Homeland Defense and Global Security:

a. Represents DoD on all homeland defense-related matters with designated lead Federal agencies, the Executive Office of the President, the Department of Homeland Security, other Executive departments and Federal agencies, and State and local entities to identify IT interoperability issues and communicate them to the DoD CIO.

b. Coordinates with DoD CIO to establish procedures to validate and resolve homeland defense-related IT interoperability requirements identified by Federal, State, and local entities external to the DoD.

## 2.11. DCAPE.

In addition to the responsibilities in Paragraph 2.13., the DCAPE:

a. Provides guidance to the MILDEPs, CCMDs, DAFAs, and other OSD Components. Approves study plans for conducting an analysis of alternatives (AoA) for major defense acquisitions programs in accordance with DoDI 5000.84 and CJCS Instruction (CJCSI) 5123.01.

b. Oversees the consideration and programming of funding to address IT interoperability requirements and resolve interoperability deficiencies for programs in sustainment as part of the AoA.

c. In coordination with the Secretaries of the MILDEPS, CCDRs, Directors of the DAFAs, and other OSD Component heads, provides recommendations to the Deputy Secretary of Defense for addressing critical IT interoperability issues through the planning, programming, budgeting, and execution process.

## 2.12. DOT&E.

In addition to the responsibilities in Paragraph 2.13., and through coordination with the Secretaries of the MILDEPs, CJCS, CCDRs, Directors of the DAFAs, and other OSD Component heads, the DOT&E:

a. Requires that joint interoperability requirements information (e.g., net-ready performance attribute and required architecture viewpoints) is addressed in operational tests as an integral part of the evaluation of the system's operational effectiveness.

b. Requires test and evaluation of IT is conducted throughout the development, procurement, and fielded phases of a system's life-cycle with sufficient frequency to accurately assess IT interoperability.

c. Ensures adequate data collection for interoperability, both instrumented and manual, are included in approved operational test plans.

d. Ensures integrated data collection across developmental and operational test events to provide shared data in support of completeness and efficiency of interoperability assessments in accordance with DoDI 5000.89.

e. In coordination with the DoD Business, Warfighting, Intelligence, and Enterprise Information Environment Warfighting Mission Area Owners (e.g., USD(I&S) and DoD CIO), requires capability-focused, architecture-based measures of performance and associated metrics to be developed in support of evaluations for IT interoperability throughout a system's life-cycle in accordance with DoDI 5000.89.

f. Assists the TRMC with developing and maintaining the proper tools and testing infrastructure to include a distributed operationally representative joint test environment to support the development and evaluation of interoperable IT.

g. Assists the MILDEPs, CCMDs, DAFAs, and OSD Components with operational test planning and assessment or evaluation of the impact of IT interoperability on operational effectiveness, suitability, and survivability.

h. Includes interoperability in the OT&E final reports' evaluation of operational effectiveness, and highlights any suitability or survivability deficiencies related to interoperability, based primarily upon end-to-end testing within an operationally representative environment.

i. Requires the development of TEMPs or equivalent documents and operational test plans, for those programs under DOT&E oversight, that identify and resource IT interoperability test requirements, in coordination with the USD(A&S), the USD(R&E), the Secretaries of the MILDEPs, the CCDRs, the Directors of the DAFAs, and other OSD Component heads.

j. Ensures the need for integrated testing and common data collection across test events to ensure completeness and efficiency in accordance with DoDI 5000.89.

k. Designates a representative to serve as an ISG special advisor.

## 2.13. OSD COMPONENT HEADS, SECRETARIES OF THE MILDEPS, CCDRS, AND THE DIRECTORS OF THE DAFAS.

The OSD Component heads, Secretaries of the MILDEPs, CCDRs, and the Directors of the DAFAs:

a. Oversee implementation of the responsibilities and procedures in this issuance within their own Component, including:

(1) Provide a Component level interoperability certification if the Joint Staff Gatekeeper determines joint net-ready certification is not applicable due to lack of joint interfaces and joint information exchanges in accordance with the JCIDS Manual.

(2) Development, review, and approval of Component IT interoperability requirements.

(3) Obtain either a joint interoperability certification, an ICTO, or a valid waiver for IT systems before connection to a DoD network.

(4) Submit AoA study plans for impending Component Milestone Decision Authorities (MDAs) to DCAPE prior to materiel development decision in accordance with DoDI 5000.85.

(5) Submit a memorandum to DCAPE certifying the MILDEPs, CCMDs, DAFAs, or OSD Components concerned are ready to start the AoA.

b. Establish procedures consistent with this issuance for component interoperability certification for IT that does not have joint interoperability requirements.

c. Establish procedures consistent with this issuance for reviewing MILDEP, CCMD, DAFA, and OSD Component IT, determining when interoperability functionality or interoperability requirements have changed, and requiring the PM to submit that IT for interoperability recertification in accordance with this issuance.

d. Designate representatives to fill the critical roles specified in Section 3, including:

(1) PMs/sponsors to execute the roles and responsibilities specified in Section 3.

(2) Authority for net-ready certification for all IT CJCS has determined not to have joint interoperability requirements, as described in Section 3.

(3) Authority for component interoperability certifications for all IT with no joint interoperability requirements.

e. Provide representatives to take part in and support the ISG.

f. Design, develop, test, evaluate, and incorporate IT interoperability into all MILDEP, CCMD, DAFA, and OSD Component IT.

(1) Require that interoperability requirements are coordinated with CJCS and the CCDRs, and that each IT system design identifies all external IT interfaces with required joint, other U.S. Government department and agency systems.

(2) Recommend tradeoffs among operational effectiveness, operational suitability, cybersecurity, survivability, and IT interoperability to USD(A&S), USD(R&E), USD(I&S), DoD CIO, and CJCS.

(3) Require IT programs to comply with the requirement for IT and NSS joint interoperability testing and certification across a system's life-cycle by planning, programming, budgeting, executing, and providing resources in accordance with agreed-to schedules and test plans and strategies. Required joint interoperability testing and certification will have some impact on schedules and costs of programs. These cost and schedule impacts will be added to the program objective memorandum and project cost estimates.

(4) Ensure that the TEMPs, or equivalent documents, for each program are aligned to the interoperability requirements, include adequate DT&E; identify sufficient resources; and outline a test and evaluation path to achieve a joint interoperability certification in a timely manner.

(5) Ensure that IT interoperability requirements are verifiable and testable.

(6) Provide to DOT&E their respective operational test agency's (OTA's) evaluation of operational effectiveness, that highlight any suitability or survivability deficiencies related to interoperability, based primarily upon end-to-end testing within an operationally representative environment.

g. Require that all initial architectural viewpoints submitted as part of interoperability requirements include the content and data required by the current version of the DoD Architecture Framework (DoDAF).

h. Require PMs to submit subsequent views, representing the same version of the system, either in accordance with the original DoDAF version used, or the most current version.

i. Ensure PMs will not be required to update architectural viewpoints solely to comply with changes in the DoDAF.

j. Ensure compliance with GEOINT policies and guidelines and provide the required self-assessments for programs that produce or distribute GEOINT.

k. Coordinate with the Director, NGA, on all GEOINT-related interoperability requirements, test strategies and plans, test and evaluation results, and joint interoperability certifications.

l. Require their CIOs to:

(1) Maintain a comprehensive list of all applicable IT systems using the designated authoritative IT registry.

(2) Oversee the development, use, and maintenance of the MILDEPs', CCMDs', DAFAs', and OSD Components' architecture, enterprise, reference, and solution that are consistent with the latest version of the DoD IEA, and support development of ISPs and the architecture viewpoints recommended in this issuance.

(3) Advise their Secretary, CCDR, Director, or OSD Component heads of alternatives and solutions to identified interoperability issues.

(4) Develop guidance to require and verify that MILDEPs', CCMDs', DAFAs' and OSD Components' IT are interoperable and supportable with other relevant IT internal and external to the aforementioned.

(5) Take part in joint ISP reviews.

m. Ensure that PMs/sponsors are responsible for making sure systems are registered in DITPR and should follow applicable Component CIO procedures and guidance.

## 2.14. CJCS.

The CJCS:

a. Provides specific guidance on preparation, format, content, timelines for submission, and review of the net-ready performance attributes.

b. Establishes policy and procedures for developing, coordinating, and certifying the net-ready performance attributes in coordination with the Secretaries of the MILDEPs, CCDRs, Directors of the DAFAs, and OSD Component heads.

c. Serves as the net-ready certification authority, as described in Section 3, for all IT with joint interoperability requirements. Determines which IT has such requirements through the requirements review process and certifies in accordance with CJCSI 5123.01.

d. In coordination with the Secretaries of the MILDEPs, CCDRs, Directors of the DAFAs, and OSD Component heads, requires and verifies the content of joint operational concepts, and

associated doctrine and operational procedures. Addresses interoperability of IT used by the Military Services and, where required, with joint and multinational forces, and other U.S. Government departments and agencies.

e. Coordinates with, and provides advice, guidance, direction, and assistance to, the OSD Component heads for IT interoperability matters.

f. In coordination with the Secretaries of the MILDEPs, CCDRs, Directors of the DAFAs, and OSD Component heads, establishes processes and procedures to present insights gained from joint operations, exercises, assessments, and experiments on IT interoperability to the ISG members.

g. Supports DoD CIO in ensuring joint interoperability requirements and related architectures include the necessary changes and updates determined through the JCIDS deliberate staffing process.

h. Designates a representative to serve as an ISG Tri-Chair and to help resolve interoperability issues.

i. Assesses interoperability in support of the ISG reviews.

j. Provides recommendations to DoD CIO on policy waiver requests.

k. Serves as the chief advocate for the CCMDs on IT interoperability.

l. Leads the U.S. Coalition Interoperability Assurance and Validation effort in support of the CCMDs to assess and resolve interoperability issues with coalition partners.

## 2.15. CCDRS.

In addition to the responsibilities in Paragraph 2.13., the CCDRs:

a. Establish additional interoperability criteria beyond those found in this issuance, if required to meet operational needs.

b. Coordinate CCMD interoperability policies, procedures, and programs with OSD and CJCS and integrate them into DoD roadmaps in emerging and fielded systems.

# SECTION 3: PROCEDURES

## 3.1. GENERAL.

The processes and procedures described in this section provide the means by which DoD CIO oversees the interoperability of IT. PMs/sponsors must identify measurable interoperability requirements for each IT in development. Requirements are validated through net-ready certification and verified through test and evaluation as part of the joint interoperability certification. The Joint Staff Command, Control, Communications, and Computers/Cyber Directorate (J-6) determines if IT has joint partner interoperability requirements in accordance with CJCSI 5123.01.

a. IT and NSS with joint interoperability requirements are within the purview of CJCS for net-ready certification and the Commander, JITC, for joint interoperability certification.

b. IT and NSS without joint interoperability requirements are within the purview of the MILDEPs, CCMDs, DAFAs, and OSD Components. These organizations are responsible for achieving net-ready and interoperability certification. They will also establish their associated test and evaluation procedures to be consistent with procedures detailed in this section.

c. PMs/sponsors will request a J-6 review to verify whether or not there are joint interoperability requirements. If not, a Joint Staff net-ready key performance parameter (KPP) "Not Applicable" certification letter will be issued to the program.

## 3.2. INTEROPERABILITY REQUIREMENTS IDENTIFICATION.

a. MILDEPs, CCMDs, DAFAs, OSD Components, and PMs/sponsors will identify interoperability requirements through:

(1) JCIDS products providing the net-ready performance attributes for IT governed by requirements established in CJCSI 5123.01.

(2) Interoperability requirements products are identified in the instructions implementing the adaptive acquisition framework pathways described in DoDI 5000.02:

(a) Major capability acquisition in accordance with DoDI 5000.85.

(b) Defense business systems (DBS) and acquisition requirements in accordance with DoDI 5000.75.

(c) Operation of the middle tier of acquisition (MTA) in accordance with DoDI 5000.80.

(d) Operation of the software acquisition in accordance with DoDI 5000.87.

(e) Functional acquisition policy in accordance with DoDIs 5000.88 and 5000.89.

(3) Other requirement products for IT not subject to CJCSI 5123.01 or the acquisition processes of DoDI 5000.02.

(4) Compliance and alignment with requirements from the applicable portions of the DoD IEA and approved subordinate reference documents. Key interoperability portions of these documents include:

(a) The business rules, standards, capability and functional measures, service interaction, sequential patterns, ontologies and taxonomies, and data views.

(b) IT standards in accordance with the GTG-F DoD IT Standards Registry (DISR), pursuant to DoDI 8310.01.

(c) Data sharing requirements and registering data sources in the appropriate registry in accordance with DoDIs 8320.02 and 8320.07.

(d) Spectrum, electromagnetic compatibility, and effective electromagnetic environmental effects requirements in accordance with DoDIs 3222.03, 4650.01, and 8320.05.

(e) Network, system resource flows, information exchanges, and technical standard requirements described in applicable peer solution architectures and governing reference architectures. The interoperability requirements are derived from applicable architecture viewpoints in accordance with the IPG.

(5) Compliance and alignment with requirements from the IPG for IT with joint interoperability requirements.

(6) DOTMLPF-P change recommendation processes in accordance with CJCSI 5123.01.

b. The MILDEPs, CCMDs, DAFAs, OSD Components, and PMs/sponsors must specify the net-ready performance attribute in the program's requirements in accordance with CJCSI 5123.01. Interoperability requirements must be succinct, measurable, and testable. The interoperability requirements must be updated and recertified throughout the IT life-cycle when changes affect interoperability (e.g., functionality, requirements, employment, and environment).

(1) CJCSI 5123.01 provides specific guidance on the preparation, format, content, and timelines for submission, review, and certification of the net-ready performance attribute.

(2) The net-ready performance attribute must:

(a) Document specific interoperability performance measures to guide system design and development.

(b) Align the system's mission(s), activities, networks, and information exchange requirements to enable the evaluation of end-to-end operational effectiveness of that exchange (e.g., information timeliness, technical exchange of information).

(3) The net-ready content must be used by the MILDEPs, CCMDs, DAFAs, and OSD Components lead DT&E organizations, aforementioned OTA, or JITC as the basis to define test

criteria to evaluate the interoperability of a given solution set. The net-ready certification should occur early so that the content can be used during all test phases.

(4) Sponsors are encouraged to use the architecture viewpoints requirements as listed in the Warfighting Mission Area Architecture Development Standard and Business Enterprise Architecture (BEA), as appropriate, when developing the net-ready content in accordance with the current version of the DoDAF.

c. For IT with joint interoperability requirements, JITC will review and comment on:

(1) The interoperability test and evaluation strategy included in the TEMP or equivalent document.

(2) Developmental test plans and provide the DT&E approval authority with an assessment of interoperability testing adequacy.

## 3.3. NET-READY CERTIFICATION PROCESS.

Net-ready certification verifies the net-ready performance attributes are correct and sufficient in scope and content to describe a system's interoperability. Net-ready certification for all IT must occur before an interoperability certification can be issued. For IT with joint or interoperability requirements, the Joint Staff will certify the program for the net-ready in accordance with the requirements outlined in the JCIDS Manual.

a. PMs/sponsors must document and submit the net-ready performance attribute for certification based on guidance provided in CJCSI 5123.01 for all IT acquisitions and procurements. MILDEPs, CCMDs, DAFAs, and OSD Components will certify net-ready performance attribute for IT without joint interoperability requirements.

b. The net-ready certification authority will record the results of the net-ready certification in the GTG-F or Knowledge Management and Decision Support System.

c. Upon significant change to system requirements, affecting interoperability, or before requesting interoperability recertification, in accordance with this issuance, PMs/sponsors will submit the net-ready performance attribute for recertification to the net-ready certification authority. This ensures that the interoperability requirements remain synchronized with current and planned operational contexts.

## 3.4. ISP PROCESS.

### a. Overview.

The ISP is a key document in achieving a joint interoperability certification. The ISP describes IT and information needs, dependencies, and interfaces for systems. It focuses on the efficient and effective exchange of information that, if not properly managed, could limit or restrict the operation of the program's IT in accordance with its defined capability.

(1) The PMs will produce an ISP in the GTG-F unless exempt by an acquisition pathway, in accordance with this issuance, for policy regarding programs that are exempt from producing ISPs.

(a) If applicable, the PMs must develop and use the ISPs to identify, resolve, and mitigate issues and risks related to the program's information infrastructure and interface requirements.

(b) The ISP must describe a system's dependencies and interface requirements in sufficient detail to enable early interoperability test and evaluation.

(c) The ISP provides key information to a system's TEMP or equivalent document.

(2) DoD CIO, CJCS, MILDEPs, CCMDs, DAFAs, and the other OSD Components use the ISP to verify compliance with policies and procedures that govern the exchange of information. The PM updates and submits the ISP for review at multiple milestones during the IT system's life-cycle to help decision makers determine if the system meets interoperability requirements. The IPG provides additional information on the ISP process.

(3) The PM revises the ISP with each submission, adding information as system functionality evolves and the solution architecture matures. The final ISP, known as the ISP of record, which describes the representative production or deployment system, must include the technical exchange of information and the operational effectiveness of that exchange of information for mission accomplishment as described in the architecture.

(4) As part of the ISP, the PM must submit architectural data in accordance with the IPG to describe the interoperability requirements of the IT. The ISP review process will assist the PM to refine these viewpoints, and result in a set of detailed, measurable interoperability criteria for use in interoperability test and evaluation.

**b. Development and Submission.**

(1) PMs/sponsors must submit the net-ready performance attribute with the required architectural data in the ISP to support interoperability test and evaluation. The ISP must include required KPPs and other key system performance attributes that specifically describe required information exchanges.

(2) PMs must develop the ISP online by entering system information through the GTG-F. The process for entering system information, content, formatting, and submission of ISP requirements is described by the GTG-F, IPG, and the applicable defense acquisition pathway guidance. Deviations from these requirements require the CJCS', MILDEPs', CCMDs', DAFAs', and OSD Components' approval.

(3) Until the GTG-F is available on the SIPRNET, unclassified "shells" of ISPs are created and submitted in the GTG-F on the Non-classified Internet Protocol Router Network in order to maintain staffing visibility and in order to be able to export a .PDF version that is organizationally tailored to the requirements of the program. The .PDF version of the ISP is then uploaded to a SIPRNET repository that is under the control of the program office or the

program's Service representative. The repository manager will then provide ISP assessor access to the classified ISP and to maintain a master comment resolution matrix. Further procedures for this are specified in the Classified Information Support Plan Assessment Guide document in the user documentation section of GTG-F.

(4) PMs submit Top Secret ISPs using a staffing notification to the appropriately classified network that includes the location of the document on the Joint Worldwide Intelligence Communications System (JWICS) and the points of contact.

(5) For IT whose requirements are governed by CJCSI 5123.01:

(a) The detailed descriptions of the net-ready performance attributes are located in the approved JCIDS document.

(b) The ISP must provide a link to, or duplicate the appropriate section(s) of, the approved requirements document that includes the certified net-ready performance attribute and the Joint Staff net-ready certification letter.

(c) For IT with joint interoperability requirements, tailoring of the required architecture viewpoints in the ISP (in accordance with the IPG) requires the Office of CJCS, MILDEPs, CCMDs, DAFAs, OSD Components, and JITC concurrence.

(d) The final ISP is submitted through the GTG-F for joint review and approval.

### c. Review and Approval.

(1) The IPG provides guidance for review of interoperability requirements for ISPs and net-ready certification to support joint interoperability testing and certification.

(2) The MILDEPs, CCMDs, DAFAs, and OSD Components will review ISPs as assigned in the GTG-F Interoperability and Supportability Assessment Module.

(3) The MILDEPs, CCMDs, DAFAs, and OSD Components are responsible for approving the final ISP of record in the GTG-F.

## 3.5. OTHER ADAPTIVE ACQUISITION FRAMEWORK PATHWAY REQUIREMENTS.

### a. Overview.

Programs that are not required to produce an ISP (i.e., if exempted) will provide information to achieve a joint interoperability certification (e.g., information needs, dependencies, interfaces for programs to support test and evaluation) using the processes and products established in the applicable acquisition pathway policies.

(1) DBS, BEA, and the Business Capability Acquisition Cycle.

DBS programs use a CIP to prepare for and manage the delivery of capability and to support statutory and regulatory requirements; it is not a specific document or set of documents. It accounts for all necessary information products required to support and inform leadership decisions.

(2) MTA.

(a) MTA rapid prototyping programs will develop a process for transitioning successful prototypes to new or existing acquisition programs for production, fielding, and operations and sustainment under the rapid fielding pathway or other acquisition pathway.

(b) MTA rapid fielding programs will develop a process for transitioning successful programs to operations and sustainment. This process will result in a transition plan, included in the acquisition strategy, which provides a timeline for completion within 2 years of all necessary documentation required for transition. Demonstrations and incremental evaluations will determine the maturity of MTA rapid fielding programs and drive the development of information requirements that will support interoperability testing and certification.

(3) Software Acquisition.

Programs using the software acquisition pathway will use a CNS to capture mission activities, enhancements to existing operational capabilities, interoperability needs, legacy interfaces, and other attributes that provide enough information to define various software solutions as they relate to the overall threat environment.

**b. Development and Submission.**

(1) PMs will develop and submit interoperability requirements for CJCS, MILDEP, CCMD, DAFA, and OSD Component approval using the formatting, content, and tools identified in applicable acquisition policies.

(2) PMs must consider the implications of compiling detailed and proprietary information in a document that receives wide distribution during review. Competition-sensitive information should be protected in accordance with appropriate guidelines.

(3) The information explains the program's concept of operations and provides IT supportability analysis of the concept of operations.

(4) Joint interoperability requirements must include the net-ready performance attribute with the required architectural data to support net-ready certification (e.g., measures, technical requirements and information exchanges) in accordance with the IPG.

(5) Repositories for submission and archiving interoperability requirements will be established as follows:

(a) For DBS, the PMs/sponsors will submit required CIP information for Joint Staff and stakeholder review through the GTG-F as needed.

(b) For software acquisitions, MILDEPs, CCMDs, DAFAs, and OSD Components will develop a streamlined process to develop, coordinate, and approve the CNS commensurate with the size, scope, risks, and urgency of needs. The software acquisition decision authorities will ensure CNS documents are available in the Knowledge Management and Decision Support System for archival and awareness purposes in accordance with DoDI 5000.87.

(c) For each MTA program, MILDEPs, CCMDs, DAFAs, and OSD Components will develop a process transitioning successful programs to operations and sustainment. This process will result in a transition plan, included in the acquisition strategy, which provides a timeline for completion within 2 years of all necessary documentation required for transition.

(6) For IT with joint requirements, PMs/sponsors are encouraged to submit unclassified interoperability products for joint review through the GTG-F. The process for staffing unclassified or classified products are covered in the IPG and in accordance with this issuance.

(7) Refer to the IPG for additional guidance on development and submission of interoperability requirements for DBS, software acquisitions, and MTA acquisition pathways.

### c. Review and Approval.

(1) The IPG provides guidance for review of interoperability requirements for the DBS, MTA, and software pathways, and net-ready certification to support joint interoperability testing and certification. The Joint Staff will determine if joint equities are involved and will execute an expedited joint review process if necessary.

(2) Refer to the CJCS', MILDEPs', CCMDs', DAFAs', and OSD Components' interoperability policy and processes for review of interoperability requirements and net-ready certification for IT that does not have joint interoperability requirements.

(3) Refer to the applicable acquisition policy for approval of acquisition pathway products.

### d. Exceptions.

Programs covered by DoDI 5000.81 do not require a joint interoperability certification.

## 3.6. IT INTEROPERABILITY TEST AND EVALUATION.

PMs must use the net-ready content to develop an integrated test and evaluation strategy (e.g., developmental testing and operational testing) to include interoperability test and evaluation, regardless of the acquisition approach. PMs must perform interoperability test and evaluation throughout system development in order to identify issues, implement solutions, and support a joint interoperability certification decision at the joint or component level.

a. The net-ready certification authority certifies the net-ready performance attribute in accordance with this issuance. Net-ready certification is not required before testing IT for interoperability; however, it reduces program risk by ensuring developers design and testers evaluate to the approved interoperability requirements.

b. PMs/sponsors (via the MILDEPs, CCMDs, DAFAs, and OSD Components) must provide the appropriate joint interoperability certification authority with the proposed interoperability test and evaluation strategy from the TEMP or equivalent document and the interoperability requirements.

c. For IT developed for a major capability acquisition, in accordance with DoDI 5000.85, the developmental testing authority will provide an assessment of DT&E to the MDA in accordance with DoDI 5000.89.

(1) This assessment must include a verification that all interoperability-related developmental testing has been completed and there are no unresolved interoperability-related problems that could cause death or injury, loss or major damage to weapons system, or decrease in the combat readiness of the using organization.

(2) Copies of those assessments should be provided to the Director, Developmental Test, Evaluation, and Assessments and the appropriate Chief DT&E authority within the MILDEPs, CCMDs, DAFAs, and OSD Components.

d. For IT developed in accordance with DBS, software acquisition, and MTA pathways, PMs/sponsors must develop tailored test strategies coordinated through JITC. These test strategies will be used to determine the frequency and scope of interoperability testing and certification. Refer to the IPG for guidance and detailed procedures.

e. For IT with joint interoperability requirements:

(1) The JITC commander or designated representative will:

(a) Participate in the system's test and evaluation working-level integrated product team or equivalent.

(b) Review and provide coordinating comments on TEMPs or equivalent documents.

(c) Collaborate with PMs/sponsors, along with developmental and operational test organizations, to address IT interoperability requirements in test plans.

(d) Leverage the information in the TEMP or equivalent document for test planning.

(2) PMs/sponsors must coordinate with JITC in the review of IT developmental and operational test plans to gain as much interoperability test data from those events as possible.

(3) PMs/sponsors of GEOINT-related IT must coordinate with NGA in the review of IT developmental, operational, and interoperability test plans to gain as much GEOINT-related test data from those events as possible.

f. For IT without joint interoperability requirements, the MILDEPs, CCMDs, DAFAs, and OSD Components will coordinate with their designated interoperability certification authorities to ensure the test and evaluation capability or activity is adequate to evaluate intra-service and intra-agency interoperability requirements.

g. The MILDEPs, CCMDs, DAFAs, and OSD Components should leverage test and evaluation capability and activities that support interoperability testing across DoD. The MILDEPs, CCMDs, DAFAs, and OSD Components should incorporate their respective test labs in the test and evaluation processes to allow more timely delivery of emerging technologies to the warfighter and business communities. Under this concept:

(1) DoD Component labs may be used for interoperability test and evaluation.

(2) Tailored test strategies developed by programs that use the DBS, software acquisition, and MTA pathways must be coordinated through JITC. These test strategies will be used to determine the frequency and scope of interoperability testing and certification. For IT with joint interoperability requirements, the MILDEPs, CCMDs, DAFAs, and OSD Components should coordinate with JITC to ensure the test and evaluation capability or activity is adequate to evaluate the joint interoperability requirements. The JITC must concur with the MILDEPs', CCMDs', DAFAs', and OSD Components' proposed interoperability test and evaluation process to ensure data is valid for a joint interoperability certification. Refer to the IPG for guidance and detailed procedures.

h. To avoid compromise of information that may reveal component or system operational limitation or vulnerabilities, results from interoperability tests, assessments, evaluations, and certifications must conform to applicable security classification guidance.

i. PMs are strongly encouraged to leverage early developmental testing to identify issues, implement solutions, assess standards conformance, and determine that the system is pursuing a viable path to interoperability.

j. Developmental testing can support a joint interoperability certification if the system and test environment are operationally relevant.

k. Testing to support a joint interoperability certification decision must replicate the system's operational network environment to the maximum extent possible.

l. The MILDEP, CCMD, DAFA, and OSD Component Chief Developmental Tester and Lead Developmental Test and Evaluation Organization must derive interoperability evaluation criteria from approved requirement sources and include it in IT test plans.

m. The DOT&E and the OTAs must develop guidelines to evaluate IT interoperability during OT&E events and joint exercises.

n. To achieve standardization and efficiency:

(1) JITC, MILDEP, CCMD, DAFA, and OSD Component stakeholders (e.g., PMs/sponsors, developmental testing organizations, and OTAs) must employ a common

evaluation framework and associated automation for interoperability requirements analysis, test planning, data analysis, reporting, and subsequent certification. (See the IPG for additional information).

(2) The TEMP or applicable acquisition pathway's test and evaluation strategy documentation must articulate the approach and resources needed to assess interoperability in accordance with DoDI 5000.89.

o. The MILDEPs, CCMDs, DAFAs, and OSD Components must:

(1) Plan, program, budget, and provide resources consistent with accepted schedules and either test plans, TEMPs, or equivalent documents. Resources include the funding, systems, equipment, processes, and personnel necessary to accomplish IT interoperability requirements and testing for joint interoperability requirements.

(2) Require comprehensive test planning (e.g., test strategies and plans) be sufficient to verify that the system meets the certified net-ready requirements (e.g., net-ready content) in accordance with the IPG.

(3) Require that the appropriate DT&E authority approve their respective TEMPs or equivalent documents for each acquisition program after verifying that adequate levels of DT&E to achieve a joint interoperability certification are planned and resourced and can be executed in a timely manner.

(4) Require that the appropriate DT&E authority review their respective test strategy and plans for each acquisition category program to ensure alignment with applicable interoperability requirements sources (e.g., ISPs, JCIDS documents) established in governing acquisition policies.

(5) Coordinate with JITC in the review of IT developmental and operational test plans.

(6) Coordinate testing to assess standards conformance and implementation requirements pursuant to DoDI 8310.01.

(7) Coordinate with NGA in the review of GEOINT-related IT developmental, operational, and interoperability test plans.

(8) Provide the results of select developmental and operational interoperability assessments, tests, and evaluations, where significant interoperability issues are observed, to the USD(A&S), the USD(R&E), DoD CIO, the DOT&E, and CJCS.

(9) Provide the MILDEPs', CCMDs', DAFAs', and OSD Components' portion of the test and evaluation infrastructure.

## 3.7. IT INTEROPERABILITY CERTIFICATION PROCESS.

### a. Overview.

Joint interoperability certification authorities will verify a system's compliance with the certified net-ready performance attribute through test and evaluation. If the system meets the threshold criteria of the net-ready requirements, joint interoperability certification authorities will certify the system for interoperability. Certification of interoperability is a significant contributor to the OTA's determination of the system's operational effectiveness, suitability, and survivability.

(1) Net-ready certification authorities must certify the net-ready performance attribute before a joint interoperability certification may be issued.

(2) PMs/sponsors must achieve a joint interoperability certification, possess an ICTO, or be granted a valid waiver to support the decision to connect an IT system to any DoD network (e.g., an approval to connect (ATC) or interim approval to connect (IATC)).

(3) PMs/sponsors ensure system(s) are recertified every 4 years or when changes potentially impact interoperability (e.g., functionality, requirements, employment, and environment), as determined by the owning MILDEPs, CCMDs, and DAFAs, in coordination with CJCS and JITC.

(4) IT initiated through a validated urgent operational need (UON) or other quick reaction capability does not require an ISP or a joint interoperability certification before network connection, unless the capability meets the threshold for a major defense acquisition program. Enclave owners may require some level of interoperability evaluation for risk mitigation purposes.

### b. Procedures.

(1) Interoperability must be assessed for certification through formal developmental and operational testing, joint exercises, or other formal assessments, and evaluated by MILDEPs, CCMDs, DAFAs, and OSD Components developmental test agencies, OTAs, the JITC, or a combination of any of these. The joint interoperability certification authority determines whether adequate test and evaluation were performed before a joint interoperability certification.

(a) JITC, as the joint interoperability certification authority for DoD IT and NSS, must develop procedures to verify, assess, and certify through testing or review of other organizations' testing, the joint interoperability of IT.

(b) Joint interoperability certification is based on the common evaluation framework. The common evaluation framework is based on the net-ready performance attribute.

(c) JITC publishes an IPG, in coordination with DoD CIO, to document procedures and information requirements (including the DoDAF architecture viewpoints) for interoperability testing and certification, waiver processing, and associated processes and procedures.

(2) Via their MILDEPS, CCMDs, DAFAs, and OSD Components, PMs/sponsors must provide the appropriate joint interoperability certification authority with the certified net-ready performance attribute.

(3) The joint interoperability certification authority must coordinate with NGA before making the joint interoperability certification decision for GEOINT-related systems.

(4) Upon completion of interoperability test and evaluation, the joint interoperability certification authority must make the joint interoperability certification decision and notify the respective PM and sponsor. For joint IT, joint interoperability certification authority can issue a joint interoperability certification, joint interoperability certification with conditions, a denial of certification, or an interoperability assessment.

(a) A joint interoperability certification is issued when IT fulfills the net-ready KPP requirements, as outlined in the JCIDS Manual, for each joint operational activity the system supports and have no critical operational impacts.

(b) A joint interoperability certification with conditions is issued for IT when only subsets of the net-ready KPP requirements are fulfilled. Conditional certifications provide the interoperability status for cases where useful capabilities are provided, despite not meeting all joint interoperability requirements, and there are no expected critical operational impacts or adverse effects on the joint interoperability environment.

1. The MDA, or other decision makers, must consider the operational risks associated with the conditions when making acquisition and fielding decisions. Conditions to a certification can be removed upon successful testing of the requirements.

2. A joint interoperability certification with conditions or a denial of certification must identify the net-ready performance attributes or threshold performance specifications that were not successfully tested (i.e., requirement not met or not tested), and assess the impact to system capabilities or mission completion.

(c) An interoperability assessment provides preliminary interoperability status. This is appropriate in cases where requirements documents are not finalized, high-risk areas warrant early feedback, etc.

(5) The joint interoperability certification authority records the joint interoperability certification decisions in the authoritative database (e.g., JITC System Tracking Program), in accordance with the IPG, and provides notice of certification and supporting information to the:

(a) MDA or any relevant fielding authority to support a fielding decision.

(b) Appropriate connection approval office (CAO) for DoD network connection approval of the ATC or IATC.

(c) ISG Tri-Chairs, members, and advisors.

### c. Recertification.

(1) PMs/sponsors must ensure their IT is reevaluated for joint interoperability certification as follows:

(a) Every 4 years.

(b) If changes occur that may impact interoperability in accordance with the IPG (e.g., functionality, requirements, employment, and environment).

(c) If certification is revoked (i.e., critical interoperability issue).

(2) PMs/sponsors will refer to the IPG for details on the recertification process.

(3) Where there is disagreement on whether a recertification is required, it will be brought before the ISG for resolution.

## 3.8. SYSTEM CONNECTION APPROVAL.

a. Once a system has completed a joint interoperability certification, the PM is authorized to apply for network connection through the appropriate enclave or network owner. The enclave or network owner must weigh the joint interoperability certifications, ICTO, waivers, OARL, and other information in deciding whether to allow connection.

b. The Secretaries of the MILDEPs, CCDRs, Director of the DAFAs, and OSD Component heads must oversee this process for connecting IT systems to enclaves owned by their respective organizations and provide appropriate guidance and procedures for PMs/sponsors to follow in accordance with DoDIs 8010.01 and 8510.01.

c. The DISA CAO must not issue or renew an ATC to an enclave unless all systems within that enclave have a valid interoperability certification, ICTO, or valid waiver. The enclave owner must submit proof of interoperability certification, ICTOs, and waivers in accordance with procedures the DISA CAO publishes. If the enclave has not met these conditions, the CAO must refer the enclave owner to the ISG, via the PM's respective ISG representative, for resolution before connection. The ISG will then provide direction to the DISA CAO to support or deny the connection request.

d. The OARL assists enclave owners by alerting them about systems not certified for interoperability that could pose an interoperability risk to other systems on the network. DISA updates and DoD CIO distributes the OARL at least quarterly to:

(1) All DoD MDAs.

(2) Affected system fielding authorities for non IT acquisition.

(3) CJCS.

(4) MILDEP, DAFA, and OSD Component CIOs.

(5) CCMD CIOs.

(6) USD(R&E).

(7) USD(A&S).

(8) DISA CAO.

## 3.9. INTEROPERABILITY GOVERNANCE.

The ISG will be subordinated to an appropriate governance forum, as determined by DoD CIO. The ISG proposes, reviews, and coordinates interoperability policies. It reviews critical interoperability issues; adjudicates requests for ICTOs, waivers to policy, and renewal of a joint interoperability certifications; and determines placement on the OARL. Representatives from DoD CIO, USD(A&S), and CJCS tri-chair the ISG, each of which will carry out specific tasks in support of the ISG as noted in Section 2. The MILDEPs, CCMDs, DAFAs, and OSD Components provide representatives to the ISG, as appropriate. The ISG charter will be signed by general officer or senior executive service representatives of DoD CIO, USD(A&S), and CJCS, and then published by DoD CIO. Representatives submit interoperability issues that cannot be resolved to ISG for resolution.

## 3.10. ICTO REQUESTS.

a. In coordination with USD(A&S) and CJCS, DoD CIO grants ICTOs for systems with joint interoperability requirements. ICTOs must only be granted when the system is progressing toward a joint interoperability certification and there is a documented need to operate the system until a joint interoperability certification can be issued.

b. PMs/sponsors submit requests for ICTOs in accordance with the IPG.

c. Each time a CAO decision is made, including renewals, the CAO must verify that any ICTOs have not expired.

## 3.11. WAIVERS TO IT INTEROPERABILITY POLICY.

a. The MILDEPs, CCMDs, DAFAs, and OSD Components may approve requests to waive the requirement for an ISP or joint interoperability certification for their respective unique (i.e., no joint interoperability requirements) IT, only if it has been determined by the Joint Staff Gatekeeper that joint net-ready certification is non-applicable. PMs/sponsors of the MILDEPs, CCMDs, DAFAs, and OSD Components must provide DoD CIO with copies of the Joint Staff net-ready non-applicable letter and their respective waiver approval memorandums.

b. PMs/sponsors must submit "waiver to policy" requests in accordance with the IPG. Only DoD CIO is authorized to approve and distribute waivers to this issuance for IT with joint interoperability requirements. In coordination with USD(A&S), USD(R&E), DOT&E, and CJCS, DoD CIO will consider waivers to this issuance only:

(1) When the operational chain of command and CJCS have validated a UON.

(2) To accommodate the introduction of new or emerging technology pilot programs that have been coordinated with, and validated by, the MILDEP, CCMD, DAFA, or OSD Component concerned.

(3) When the requesting MILDEP, CCMD, DAFA, or OSD Component can demonstrate that the cost of complying with this policy outweighs the benefit to DoD.

c. Statutory requirements may be waived only if the statute specifically provides for doing so.

d. JITC must review all requests for waivers of interoperability policy requiring DoD CIO approval, analyze those requests, and provide a recommendation to DoD CIO in accordance with the IPG.

e. Waivers may be either permanent or temporary, at the discretion of DoD CIO.

# GLOSSARY

## G.1. ACRONYMS.

| ACRONYM | MEANING |
|---|---|
| AoA | analysis of alternatives |
| ATC | approval to connect |
| BEA | business enterprise architecture |
| CAO | connection approval offices |
| CCDR | Combatant Commander |
| CCMD | Combatant Command |
| CI | counterintelligence |
| CIO | chief information officer |
| CIP | capability implementation plan |
| CJCS | Chairman of the Joint Chiefs of Staff |
| CJCSI | Chairman of the Joint Chiefs of Staff instruction |
| CNS | capability needs statement |
| DAFAs | Defense Agencies and DoD Field Activities |
| DBS | defense business systems |
| DCAPE | Director of Cost Assessment and Program Evaluations |
| DIA | Defense Intelligence Agency |
| DIRNSA/CHCSS | Director, National Security Agency/Chief, Central Security Service |
| DISA | Defense Information Systems Agency |
| DISR | DoD Information Technology Standards Registry |
| DITPR | DoD Information Technology Portfolio Repository |
| DNI | Director of National Intelligence |
| DoDAF | DoD Architecture Framework |
| DoD CIO | DoD Chief Information Officer |
| DoDD | DoD directive |
| DoD IEA | DoD Information Enterprise Architecture |
| DoDI | DoD instruction |
| DOT&E | Director of Operational Test and Evaluation |
| DOTMLPF-P | doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy |
| DT&E | developmental test and evaluation |
| GEOINT | geospatial intelligence |
| GTG-F | Global Information Grid Technical Guidance Federation |
| IATC | interim approval to connect |
| IC | intelligence community |
| ICTO | interim certificate to operate |

| ACRONYM | MEANING |
|---|---|
| IPG | Interoperability Process Guide |
| ISG | Interoperability Steering Group |
| ISP | information support plan |
| IT | information technology |
| J-6 | (Joint Staff) Command, Control, Communications, and Computers/Cyber Directorate |
| JCIDS | Joint Capabilities Integration and Development System |
| JITC | Joint Interoperability Test Command |
| JWICS | Joint Worldwide Intelligence Communications System |
| KPP | key performance parameter |
| MDA | Milestone Decision Authority |
| MILDEP | Military Department |
| MTA | middle tier of acquisition |
| NGA | National Geospatial-Intelligence Agency |
| NSA/CSS | National Security Agency/Central Security Service |
| NSS | national security systems |
| OARL | operating at risk list |
| OT&E | operational test and evaluation |
| OTA | operational test agency |
| PDF | portable document format |
| PM | program manager |
| SIGINT | signals intelligence |
| SIPRNET | SECRET Internet Protocol Router Network |
| TEMP | test and evaluation master plan |
| TRMC | Test Resource Management Center |
| UON | urgent operational need |
| USD(A&S) | Under Secretary of Defense for Acquisition and Sustainment |
| USD(I&S) | Under Secretary of Defense for Intelligence and Security |
| USD(R&E) | Under Secretary of Defense for Research and Engineering |

## G.2. DEFINITIONS.

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

| TERM | DEFINITION |
|---|---|
| **acquisition categories** | Categories of DoD acquisition programs established to facilitate decentralized decision making as well as execution and compliance with statutorily imposed requirements. The categories indicate the level of review, decision authority, and applicable procedures. |
| **architecture** | The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. |
| **assessment (assess)** | The act or result of determining the contribution or disposition of an activity, product, or condition, based on an appraisal of the state of IT interoperability. |
| **ATC** | A formal statement by the appropriate CAO granting approval for an information system to connect to a DoD network. |
| **authoritative IT registry** | The DoD CIO-designated enterprise database containing descriptive information for IT. |
| **BEA** | A strategic information asset base that defines the business missions, the information and technologies necessary to perform those missions, and the transitional processes for implementing new technologies in response to changing mission needs. This includes the baseline architecture, a target architecture, and a sequencing plan. In the DoD, the BEA is the blueprint to guide and constrain investments by the DoD and OSD Components as they relate to or impact business operations. |
| **CAO** | An office responsible for reviewing and approving all connection requests and issuing ATCs and IATCs for a given DoD network. |
| **capability** | The ability to execute a specified course of action. A capability may or may not be accompanied by an intention. |
| **capability gap** | The inability to execute a specified course of action. The gap may be the result of no existing capability, lack of proficiency or sufficiency in an existing capability solution, or the need to replace an existing capability solution to prevent a future gap. |
| **CIP** | An aggregation of the content needed by the program office to prepare for and manage the delivery of the capability and to support statutory and regulatory requirements; it is not a specific document or set of documents. It accounts for all necessary information products required to support and inform leadership decisions. |

| TERM | DEFINITION |
|---|---|
| **CNS** | A high-level capture of mission deficiencies, or enhancements to existing operational capabilities, features, interoperability needs, legacy interfaces, and other attributes that provide enough information to define various software solutions as they relate to the overall threat environment. |
| **cybersecurity** | Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation. |
| **DBS** | Defined in DoDI 5000.75 as "business system." |
| **DISR** | A registry of IT standards which are selected through a defined governance process. It contains the minimal set of rules governing the arrangement, interaction, and interdependence of IT system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. It defines the service areas, interfaces, standards, and standards profiles applicable to all DoD systems. Use of the DISR is mandated for the development and acquisition of new or modified fielded IT systems throughout the DoD. The standards cited in the DISR replaced the Joint Technical Architecture. |
| **DITPR** | The DoD's authoritative inventories of IT systems. It provides senior DoD decision makers a coherent and contextual view of the capabilities and associated system enablers for making resource decisions and a common central repository for IT system information to support the certification processes of the various Investment Review Boards and the DBS Management Committee. |
| **DoD IEA** | Defined in DoDD 8000.01. |
| **DT&E** | A process that provides PMs and decision makers with knowledge to measure progress and characterize system capabilities and limitations. Programs conduct DT&E throughout the system's life-cycle, from program initiation through system sustainment, to reduce design and programmatic risks and provide assessments. DT&E occurs as contractor testing and government testing or a mix of both. |

| TERM | DEFINITION |
|---|---|
| **enclave** | Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. |
| **end-to-end testing** | The logical means to conduct a mission-based evaluation. End-to-end testing is easiest thought of as testing a mission thread. Mission threads result from a careful analysis of a unit's mission using the system and can be derived from the joint mission essential task list, from the Component-specific mission essential task list, concept of employment, or the Army's operational mission summary and mission profile. The threads should make operational sense and evaluate the intended operational mission from beginning to end. The end-to-end evaluation of each mission thread should rely on testing that includes the entire thread in a single operational event. |
| **enterprise architecture** | The explicit description and documentation of the current and desired relationships among business and management processes and IT. |
| **evaluation (evaluate)** | Measuring or quantifying the value, characteristics, or capabilities of something against established standards, as in "test and evaluation." The determination of or act of determining the relative degree to which IT interoperability is achieved. |
| **GTG-F** | Operated and maintained by DISA, a federated suite of tools utilized by the interoperability and supportability joint community to develop, manage, reference, or assess various artifacts such as ISPs, the net-ready performance attributes, architecture products, and DoD IT standards. For more information, visit https://gtg.csd.disa.mil/. |
| **IATC** | Temporary approval granted by the appropriate CAO for the connection of an information system to a DoD network under the conditions or constraints enumerated in the connection approval. |
| **ICTO** | A temporary authorization to proceed to connection without completing full joint interoperability certification. Issued by the ISG to PMs who have an urgent need to operate IT, have not completed joint interoperability certification, but are making satisfactory progress towards that goal as determined by the ISG. |

| TERM | DEFINITION |
|---|---|
| **information requirements** | A condition or situation requiring knowledge or intelligence derived from received, stored, or processed facts and data. |
| **information system** | Computer-based information systems are complementary networks of hardware and software that people and organizations use to collect, filter, process, create, and distribute data. |
| **information timeliness** | Occurring at a suitable or appropriate time for a particular condition or situation. |
| **interoperability** | The ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces, and to use the data, information, materiel, and services exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment in its operational environment including appropriate cybersecurity aspects. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions in appropriately stressed operational environments over the system's life-cycle. |
| **interoperability requirements** | The document or collection of documents or products (e.g., net-ready performance attribute, ISP, CIP) that establish the testable measures, conditions, criteria and standards used to evaluate interoperability of a capability based on the interoperability evaluation framework. Joint interoperability requirements are currently aligned with the net-ready performance attribute. |
| **ISP** | A set of information supporting interoperability test and certification. It is entered through the GTG-F and the ISP contains or links the net-ready performance attribute along with supporting architectural data. Instructions for completion of the ISP are found on the GTG-F. The IPG provides additional information on the ISP. |

| TERM | DEFINITION |
|---|---|
| **IT** | Any equipment or interconnected system or subsystem of equipment, used in automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources. |
| **IT architecture** | Architecture of an enterprise's IT (see "architecture"). |
| **IT service** | The performance of any work related to IT and the operation of IT, including NSS. This includes outsourced IT-based business processes, outsourced IT, and outsourced information functions. |
| **JCIDS** | A CJCS process identifying, assessing, and prioritizing joint military capability needs. The JCIDS process is a collaborative effort, which uses joint concepts and DoD architectures to identify prioritized capability gaps and integrated DOTMLPF-P solutions (materiel and non-materiel) to resolve those gaps. JCIDS is fully described in CJCSI 5123.01. |
| **joint interoperability certification** | A formal statement of adequacy, provided by the responsible joint interoperability certification authority agency, that a system has met its joint interoperability requirements. |
| **joint interoperability certification authority** | The office with the certification authority for the interoperability. It verifies that the IT has met its joint interoperability requirements, as proven through test and evaluation. For IT with joint interoperability requirements, the joint interoperability certification authority is JITC. For all other IT, the owning MILDEPs, CCMDs, DAFAs, and OSD Components designate the interoperability certification authority. |
| **joint interoperability requirements** | Any requirement levied on an IT to implement information exchanges to other IT across or beyond a MILDEP's, a CCMD's, DAFAs', and an OSD Component's boundaries or implement a web service with the explicit or implicit intention to share information with other IT across or beyond their boundaries. |
| **KPPs** | Minimum attributes or characteristics considered most essential for an effective military capability. |

| TERM | DEFINITION |
|---|---|
| **MDA** | The designated individual with overall responsibility for a program. The MDA has the authority to approve entry of an acquisition program into the next phase of the acquisition process and is accountable for cost, schedule, and performance reporting to a higher authority, including congressional reporting. For interoperability purposes, the MDA uses the information and recommendations of the net-ready certification authority and interoperability certification authority to decide if a system is ready to move to the next acquisition milestone. |
| **milestones** | Major decision points that separate the phases of an acquisition program. |
| **MTA** | Defined in DoDI 5000.02. |

| TERM | DEFINITION |
|---|---|
| **net-ready** | DoD IT that meets required information needs and information timeliness requirements, has a cybersecurity accreditation, and meets the attributes required to support military operations, to be entered and managed on the network, and to effectively exchange information for both the technical exchange of information and the operational effectiveness of that exchange.<br><br>DoD IT that is net-ready enables warfighters and DoD business operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all participants.<br><br>Net-readiness requires that IT operate in an environment where there exists a distributed information processing environment in which applications are integrated; applications and data independent of hardware are integrated; information transfer capabilities exist to ensure communications within and across diverse media; information is in a common format with a common meaning; common human-computer interfaces for users and effective means to protect the information exist.<br><br>Net-readiness is critical to achieving the envisioned objective of a cost-effective integrated environment. Achieving and maintaining this vision requires interoperability within a joint task force or CCMD area of responsibility; across CCMD area of responsibility boundaries; between strategic and tactical systems; within and across Military Services and agencies; from the battlefield to the sustaining base; among U.S., allied, and coalition forces; and across current and future systems. |
| **net-ready certification** | An authoritative act or process of supporting or validating whether IT interoperability requirements are appropriate and complete. |
| **net-ready certification authority** | The office with the authority to certify net-ready content. It verifies that the PM/sponsor has properly scoped, refined, and justified the interoperability requirements of the system. The CJCS is the net-ready certification authority and may delegate this authority to the appropriate MILDEPs, CCDRs, DAFAs, and OSD Components for all IT with no joint interoperability requirements. |

| TERM | DEFINITION |
|---|---|
| **net-ready KPP** | Assesses information requirements, information timeliness, and net ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. Consists of testable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given system. |
| **net-ready performance attribute** | Ensures interoperability between individually developed and fielded capability solutions as outlined in the JCIDS Manual. |
| **NSS** | Defined in Section 3552(b)(6) of Title 44, United States Code. |
| **OARL** | A watch list for critical IT and NSS systems having significant interoperability deficiencies requiring DoD oversight toward achieving and maintaining interoperability as defined in the IPG. |
| **OTA** | Organizations performing OT&E within the DoD, specifically the Army Test and Evaluation Command, the Navy Operational Test and Evaluation Force, the Air Force Operational Test and Evaluation Center, the Marine Corps Operational Test and Evaluation Activity, and JITC. |
| **PM** | The person tasked with developing and fielding the new IT system. |
| **reference architecture** | An authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions. |
| **SIGINT** | A category of intelligence, comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation SIGINT. |
| **software acquisition** | Defined in DoDI 5000.87. |
| **solution architecture** | Describes and documents a solution for a given problem driven by requirements. It describes the fundamental organization of a solution, relationships, and the principles governing its design and evolution. |

| TERM | DEFINITION |
|---|---|
| **test and evaluation** | Process by which a system or components are exercised and results analyzed to provide performance-related information. The information has many uses including risk identification and risk mitigation. Test and evaluation enables an assessment of the system's attainment of the technical performance, specifications, and system maturity. |
| **UON** | Defined in CJCSI 5123.01. |
| **warfighting mission area** | Defined in DoDI 8115.02. |
| **working-level integrated product team** | An integrated test team that consists of empowered representatives of test data producers and consumers including all applicable stakeholders to ensure collaboration and to develop a strategy for robust, efficient testing to support systems engineering, evaluations, and certifications throughout the acquisition life-cycle. |

# REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 5123.01, "Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)," October 30, 2021

Committee on National Security Systems Policy No. 15, "Use of Public Standards for Secure Information Sharing," October 20, 2016

DoD Digital Modernization Strategy, "DoD Information Resource Management Strategic Plan FY 19-23," July 12, 2019

DoD Directive 5000.01, "The Defense Acquisition System," September 9, 2020, as amended

DoD Directive 5105.71, "Department of Defense Test Resource Management Center (TRMC)," March 8, 2004

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Instruction 3222.03, "DoD Electromagnetic Environmental Effects (E3) Program," August 25, 2014, as amended

DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009, as amended

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020

DoD Instruction 5000.75, "Business Systems Requirements and Acquisition," February 2, 2017, as amended

DoD Instruction 5000.80, "Operation of the Middle Tier of Acquisition (MTA)," December 30, 2019

DoD Instruction 5000.81, "Urgent Capability Acquisition," December 31, 2019

DoD Instruction 5000.84, "Analysis of Alternatives," August 4, 2020

DoD Instruction 5000.85, "Major Capability Acquisition," August 6, 2020, as amended

DoD Instruction 5000.87, "Operation of the Software Acquisition Pathway," October 2, 2020

DoD Instruction 5000.88, "Engineering of Defense Systems," November 18, 2020

DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020

DoD Instruction 8010.01, "Department of Defense Information Network (DODIN) Transport," September 10, 2018

DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010

DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006

DoD Instruction 8310.01, "Information Technology Standards in the DoD", February 2, 2015, as amended

DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013, as amended

DoD Instruction 8320.05, "Electromagnetic Spectrum Data Sharing," August 18, 2011, as amended

DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense," August 3, 2015, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended

Executive Order 13231, "Critical Infrastructure Protection in the Information Age," October 16, 2001, as amended

Executive Order 13526, "Classified National Security Information," December 29, 2009

Global Information Grid Technical Guidance Federation Website, "DoD IT Standards Registry Online," current edition[1]

Joint Interoperability Test Command, "Interoperability Process Guide," Version 2.0, March 23, 2015, as amended

Knowledge Management and Decision Support System, Version 2, August 15, 2018[2]

Manual for the Operation of the Joint Capabilities Integration and Development System, October 30, 2021

Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 19, 2017

Office of the DoD Chief Information Officer, "DoD Digital Modernization Strategy," March 29, 2019

Office of the DoD Chief Information Officer, "DoD Information Enterprise Architecture," current edition

Office of the DoD Deputy Chief Information Officer, "DoD Architecture Framework," current edition

Operational Test and Evaluation, "Test and Evaluation Master Plan (TEMP) Guidebook," Version 3.1, January 19, 2017

United States Code, Title 10

United States Code, Title 40

United States Code, Title 44, Section 3552(b)(6)

[1] Available to Common Access Card holders at https://gtg.csd.disa.mil/uam/support/userDocument/list.
[2] Available on the SIPRNET at https://jrockmdsbpm.js.smil.mil. Registration is required for access.