# Department of Defense
# INSTRUCTION

**NUMBER** 8330.01
May 21, 2014
*Incorporating Change 1, December 18, 2017*

DoD CIO

SUBJECT: Interoperability of Information Technology (IT), Including National Security Systems (NSS)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)) and the guidance in DoDD 8000.01 (Reference (b)):

(1) Establishes policy, assigns responsibilities, and provides direction for certifying the interoperability of IT and NSS pursuant to sections 2222, 2223, and 2224 of Title 10, United States Code (Reference (c)).

(2) Establishes a capability-focused, architecture-based approach for interoperability analysis.

(3) Establishes the governing policy and responsibilities for interoperability requirements development, test, certification and prerequisite for connection of IT, including NSS (referred to in this instruction as "IT").

(4) Defines a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) approach to enhance life-cycle interoperability of IT.

(5) Establishes the requirement for enterprise services to be certified for interoperability.

b. Incorporates and cancels DoDD 4630.05, DoDI 4630.8, and DoD Chief Information Officer (CIO) memorandum (References (d), (e), and (f)).

2. APPLICABILITY

a. This instruction applies to:

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

*(2) The United States Coast Guard. The U.S. Coast Guard will adhere to DoD requirements, standards, and policies in this instruction in accordance with the direction in Paragraph 4a of the Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security (Reference (af)).*

(~~2~~*3*) All IT (systems, applications, products or IT services) any DoD Component acquires, procures, or operates, including IT that:

(a) DoD intelligence agencies, DoD Component intelligence elements, and other DoD intelligence activities engaged in direct support of DoD missions, acquire, procure (systems or services), sponsor, or operate.

(b) The Combatant Commanders, their Commands, and subordinate commands acquire, procure, or operate. 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).

(c) Shares, exchanges, or uses information to enable units or forces to operate in joint, multinational, and interagency operations.

(d) Supports all DoD mission areas as defined in DoDI 8115.02 (Reference (g)).

(e) Provides enterprise services to enable units or forces to operate in joint, multinational, and interagency operations.

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

b. This instruction does **not** apply to IT:

(1) That only performs the functions of simulation or training and only stores, processes, or exchanges simulated (i.e., not real-world) data, and has no possibility of exporting data into an operational system.

(2) That is used exclusively for demonstration or simulation, imports but does not export real-world data, and does not use that data to support any operational (e.g., warfighting, business, intelligence, enterprise information environment) process or decision making.

(3) That is designated as DoD unified capabilities (UC) and is governed in accordance with DoDI 8100.04 (Reference (h)).

3. POLICY. It is DoD policy that:

a. IT that DoD Components use must interoperate, to the maximum extent practicable, 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. All IT, including defense acquisition and procurement programs and enterprise services, must have a net ready key performance parameter (NR KPP) as part of its interoperability requirements documentation. The NR KPP consists of measurable and testable performance measures and metrics derived from associated DoD architectures, and is used to assess both the technical exchange of information, data, and services, and the end-to-end operational effectiveness of those exchanges.

c. IT interoperability must be evaluated early and with sufficient frequency throughout a system's life cycle to capture and assess changes affecting interoperability in a joint, multinational, and interagency environment. Interoperability testing must be comprehensive, cost effective, and completed, and interoperability certification granted, before fielding of a new IT capability or upgrade to existing IT.

d. IT must be certified for interoperability, or possess an interim certificate to operate (ICTO) or waiver to policy in accordance with section 9 of Enclosure 3, before connection to any DoD network (other than for test purposes).

e. Special measures may be required for protection and handling of foreign intelligence or counterintelligence information, or other need-to-know information, particularly when it contains information concerning U.S. persons. Accordingly, execution of this instruction must be tailored to comply with coordinated Director of National Intelligence (DNI) directives, Intelligence Community (IC) policies, and DoD intelligence policies.

f. This instruction 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 (References (i) and (j)), national security information systems pursuant to Executive Order 13231 (Reference (k)), and other laws and regulations.

g. Nothing in this instruction replaces or modifies the cybersecurity (formerly information assurance (IA)) requirements of DoDI 8500.01 (Reference (l)) and DoDI 8510.01 (Reference (m)). All IT developers and operators must fully comply with those instructions as well.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. ~~**Unlimited**. This instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.~~ ***Cleared for public release.*** *This instruction is available on the Directives Division Website at http://www.esd.whs.mil/DD/*.

7. EFFECTIVE DATE. This instruction~~:~~ *is effective May 21, 2014.*

~~a. Is effective May 21, 2014.~~

~~b. Must be reissued, cancelled, or certified current within 5 years of its publication to be considered current in accordance with DoD Instruction 5025.01 (Reference (n)).~~

~~c. Will expire effective May 21, 2024 and be removed from the DoD Issuances Website if it hasn't been reissued or cancelled in accordance with Reference (n).~~

David L. De Vries
Acting Department of Defense
Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

FIGURE

ENCLOSURE 1

REFERENCES

~~(a) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," April 22, 2013~~
*(a) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended*
(b) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009*, as amended*
(c) Title 10, United States Code
(d) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004 (hereby cancelled)
(e) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004 (hereby cancelled)
(f) DoD Chief Information Officer Memorandum, "Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)," March 27, 2012 (hereby cancelled)
(g) DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006
(h) DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010
(i) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(j) Executive Order 13526, "Classified National Security Information," December 29, 2009
(k) Executive Order 13231, "Critical Infrastructure Protection in the Information Age," October 16, 2001, as amended
(l) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(m) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014*, as amended*
~~(n) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012, as amended~~
(o) Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Chief Information Officer (CIO) Executive Board Charter," February 12, 2012
(p) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003, as amended
~~(q) Interim DoD Instruction 5000.02, "Operation of the Defense Acquisition System," November 25, 2013~~
*(q) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, as amended*
(r) Committee on National Security Systems (CNSS) Policy No. 15, "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems," October 1, 2012[1]
(s) DoD ~~Directive~~ *Instruction* 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
(t) DoD Architecture Framework, Version 2.02, August 2012[2]

[1] Please contact the CNSS office at cnss@nsa.gov to obtain a copy of this document.
[2] Available at: http://dodcio.defense.gov/dodaf20.aspx.

(u) DoD Information Enterprise Architecture 2.0, August 10, 2012[3]
(v) Joint On-Demand Interoperability Network Lab[4]
(w) Chairman of the Joint Chiefs of Staff Instruction 3170.01H, "Joint Capabilities Integration and Development System," January 10, 2012
(x) Global Information Grid Technical Guidance Federation Website, "DoD IT Standards Registry Online"[5]
~~(y) DoD 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006~~
*(y) DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense," August 3, 2015*
(z) DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009*, as amended*
(aa) DoD Instruction 8320.05, "Electromagnetic Spectrum Data Sharing," August 18, 2011
(ab) Chairman of the Joint Chiefs of Staff Instruction 6212.01F, "Net Ready Key Performance Parameter (NR KPP)," March 21, 2012
(ac) Defense Acquisition Guidebook Website[6]
(ad) Title 40, United States Code
(ae) Title 44, United States Code
*(af) 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*[7]

[3] Available at: http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx.
[4] Available at: https://www.us.army.mil/suite/page/510535
[5] Available at: https://gtg.csd.disa.mil/
[6] Available at: https://dag.dau.mil/
*[7] Available at https://dcms.uscg.afpims.mil/Our-Organization/Assistant-Commandant-for-C4IT-CG-6-/The-Office-of-Information-Management-CG-61/Interagency-Agreements/*

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CIO. In addition to the responsibilities in section 12 of this enclosure, the DoD CIO:

a. Maintains this instruction in coordination with the other OSD and DoD Component heads.

b. Provides oversight of IT interoperability, in coordination with the DoD Components and other mission partners.

c. Establishes policy 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) Adjudicating waivers to this instruction and requests for ICTOs for IT with joint, multinational, and interagency interoperability requirements as found in section 9 of Enclosure 3 of this instruction.

d. Maintains the DoD Enterprise Architecture (EA) in accordance with Reference (b).

e. Requires and verifies, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the CJCS, the Deputy Chief Management Officer (DCMO), and the other DoD Component heads, that DoD architectures (enterprise, reference and solution) are defined, developed, integrated, coordinated, validated, synchronized, and used.

f. Requires that IT architecture (enterprise, reference and solution) data is sufficient to assess interoperability.

g. Establishes responsibilities and procedures, in coordination with the USD(AT&L), the Director of Operational Test and Evaluation (DOT&E), the CJCS, the DCMO, and the other DoD Component heads, to require appropriate interoperability assessment and reassessment throughout a system's life cycle. In coordination with the DoD Components, oversees the establishment of measurable and testable certification criteria for interoperability assessment.

h. Maintains liaison with the CIO of the Intelligence Community within the Office of the DNI to identify and resolve DoD and IC interoperability issues.

i. Designates the authoritative IT registry (or registries) for the DoD, and publishes procedures for registering all DoD IT within the registry (or registries).

j. Establishes the IT Interoperability Steering Group (ISG), subordinate to the appropriate forum of the DoD CIO Executive Board (EB) as determined by the DoD CIO and described in its charter (Reference (o)). Designates a representative to serve as ISG tri-chair along with USD(AT&L) and CJCS representatives (for details on ISG structure and functions, see section 8 of Enclosure 3 of this instruction). Publishes and maintains the ISG charter.

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

(1) Establishes, in coordination with the USD(AT&L), the DOT&E, the CJCS, and the other DoD Mission Area Owners (DCMO and the Office of the Under Secretary of Defense for Intelligence (OUSD(I))) process, procedures, format, and content guidance for developing and submitting ISPs on acquisition category (ACAT), non-ACAT, and fielded IT.

(2) Coordinates with DoD Components in establishing ISP review processes to support joint reviews of DoD Component systems.

(3) Adjudicates critical comments in joint ISP reviews that cannot be resolved at the DoD Component level.

l. Addresses specific recommendations for critical IT interoperability issues within the DoD CIO annual Defense Planning Guidance to the DoD Components that support the future planning, programming, budgeting, and execution cycle.

m. Provides policy and oversight for requiring and achieving the interoperability of enterprise services.

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

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in section 12 of this enclosure, the Director, DISA:

a. Conducts the joint, multinational, and interagency IT interoperability assessment, test, and evaluation program, in collaboration with the other DoD Components.

b. Operates and maintains the Global Information Grid Technical Guidance Federation (GTG-F) online portal at https://gtg.csd.disa.mil and associated processes supporting the preparation, submission, verification, assessment review, and approval of ISPs.

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

d. Provides systems engineering, planning, and program guidance, in coordination with the USD(AT&L). Aids the DoD Components with developmental IT interoperability testing to deliver solutions, reduce duplication of effort, and enhance IT interoperability.

e. Maintains the Operating At Risk List (OARL), listing all IT systems that were denied an ICTO, are operating on a DoD network without interoperability certification or ICTO, and have not received an appropriate waiver to this instruction.

f. Defines the strategy and process for the interoperability test and certification of enterprise services within DoD.

g. Enforces the requirement for interoperability certification or granting of an ICTO before connection to the Defense Information Systems Network (DISN) through the DISN connection approval process.

h. Builds and delivers the Mobility EA to provide interoperable, secure (classified and unclassified) mobile communications capabilities to the DoD on a global basis.

i. Defines and executes the strategy, processes, and reference architectures to enhance the interoperability of enterprise services within the DoD.

j. Establishes a standard approach for evaluation of critical exchange points between enterprise services, infrastructures, and environments using measures of performance (MOPs) and measures of effectiveness (MOEs). Confirms interoperability from end-to-end in a multi-vendor, multi-networked, and multi-service environment.

k. Reviews and comments on interoperability test criteria for and leads execution of interoperability assessments across the DoD mobility program.

l. Reviews and comments on interoperability test criteria for and execution of interoperability assessments for IT supporting cyberspace operations.

m. Coordinates with Director, NGA on all geospatial intelligence (GEOINT)-related interoperability certifications.

n. Directs the DISA Joint Interoperability Test Command (JITC) to:

(1) Evaluate and certify joint, multinational, and interagency IT interoperability for the DoD.

(2) Serve as the Interoperability Certification Authority for all DoD IT with joint, multinational, or interagency interoperability requirements, as described in Enclosure 3 of this instruction.

(3) Establish, in coordination with the DoD CIO, the USD(AT&L), the DOT&E, the DCMO, and the other DoD Component heads, procedures to verify, assess, and certify, through testing, joint, multinational, and interagency IT interoperability throughout a system's life cycle.

(4) Publish and maintain an Interoperability Process Guide (IPG) outlining all procedures required to support joint, multinational, and interagency interoperability test and certification, ICTO requests, and waiver submissions.

(5) Review and provide recommendations on requests for waiver of interoperability policy as described in section 9 of Enclosure 3 of this instruction.

(6) Coordinate with the DoD Components to resolve joint, multinational, or interagency IT interoperability issues. If resolution cannot be achieved, provide an impact statement and recommendations for resolution to the ISG.

(7) Participate in the Joint Capabilities Integration and Development System (JCIDS) review to verify that the NR KPP is adequately defined to support interoperability testing.

(8) In coordination with program managers (PMs) of IT with joint, multinational, or interagency interoperability requirements, review Test and Evaluation Master Plans (TEMPs), and associated developmental and operational test plans for interoperability.

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

(10) Provide, in support of developmental test and evaluation (DT&E) assessments and operational test readiness reviews, for all DoD IT with joint, multinational, or interagency interoperability requirements:

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

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

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

(11) Define the methodology to test and certify enterprise services for interoperability within the DoD.

(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 enterprise service must meet before fielding.

(13) Lead the U.S. Coalition Interoperability Assurance and Validation effort in support of CCMDs to assess and resolve interoperability issues with mission partners.

3. USD(AT&L). In addition to the responsibilities in section 12 of this enclosure, the USD(AT&L):

a. Incorporates the policies and requirements in this instruction into the DoD documents governing acquisition (including DoDD 5000.01 (Reference (p)) and DoDI 5000.02 (Reference (q))), and adequately addresses this guidance during system acquisitions, as the DoD Acquisition Executive (pursuant to section 133 of Reference (c)).

b. Approves tradeoffs among operational effectiveness, operational suitability, and interoperability, for all USD(AT&L) oversight ACAT acquisition and procurement matters pertaining to IT, in coordination with the DoD CIO and the CJCS.

c. Manages acquisition of Major Defense Acquisition Program-related and Major Automated Information System program-related IT and aids the DoD CIO, the DOT&E, the DCMO, the CJCS, and the other DoD Component heads in the evaluation of interoperability requirements in both a technical and an operational context.

d. Requires, in coordination with the DoD Business, Warfighting, Intelligence, and Enterprise Information Environment Mission Area Owners (DCMO, JCS, OUSD(I), and DoD CIO), and the other DoD Component heads, that operationally prioritized materiel and non-materiel interoperability requirements are phased for acquisition and fielding.

e. Requires, in coordination with the DoD CIO and the CJCS, that IT interoperability requirements, as described in the ISP, are verifiable and testable as part of the acquisition and procurement processes.

f. Directs the Deputy Assistant Secretary of Defense for DT&E (DASD(DT&E)) to establish, and co-chair with the DOT&E, the Interoperability Test and Evaluation Panel (ITEP).

g. Establishes the architecture for a DoD enterprise-wide interoperability test capability, which must include an operationally representative joint test environment. Requires and verifies that DoD Component investments for test are consistent with this test capability. For investments determined not to be consistent, coordinates with the responsible DoD Component on a mutually satisfactory set of corrective actions before investments may proceed.

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

i. Designates a representative to serve as ISG tri-chair together with DoD CIO and CJCS representatives (for details on ISG structure and functions, see section 8 of Enclosure 3 of this instruction).

j. Establishes procedures ensuring that the appropriate DT&E authority approves TEMPs, or equivalent documents, for each ACAT program after verifying that adequate levels of DT&E to achieve interoperability certification are planned, resourced, and can be executed in a timely manner.

4. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/ CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO)). In addition to the responsibilities in section 12 of this enclosure, the USD(C)/CFO:

a. Addresses, in coordination with the other DoD Component heads, IT interoperability resource issues resulting from the requirements of this instruction in the budgetary process.

b. Provides the Deputy Secretary of Defense, in coordination with the USD(AT&L), the USD(I), the DoD CIO, the CJCS, and the other DoD Component heads, budget recommendations for addressing critical IT interoperability issues identified through the interoperability governance process.

5. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND ~~AMERICAS' SECURITY AFFAIRS~~ *GLOBAL SECURITY* (ASD(HD&~~ASA~~*GS*)). Under the authority, direction, and control of the Under Secretary of Defense for Policy and in addition to the responsibilities in section 12 of this enclosure, the ASD(HD&~~ ASA~~*GS* ):

a. Represents the 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. Establishes procedures, in coordination with the DoD CIO, to assess and verify homeland defense-related IT interoperability requirements identified by federal, State, and local entities external to the DoD are valid.

6. DCMO. In addition to the responsibilities in section 12 of this enclosure, the DCMO:

a. Ensures business systems and business improvement policies and programs are efficiently and effectively designed, executed, and aligned with DoD strategy to ensure system and process integration, and interoperability across all DoD mission areas.

b. Leads end-to-end integration and improvement of business systems and business operations in support of national security.

c. Is responsible for the DoD Business Enterprise Architecture (BEA), Strategic Management Plan, Investment Review Process, and Enterprise Transition Plan along with other DoD products, services, and publications focused on delivering integrated and interoperable business operations that support and enable the warfighter.

7. DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION (DCAPE). In addition to the responsibilities in section 12 of this enclosure, the DCAPE:

a. Provides guidance to the DoD Components for conducting an analysis of alternatives (AoA) for IT capability gaps identified through the JCIDS or Business Capability Lifecycle (BCL) process.

b. Oversees the consideration and addressing of IT interoperability requirements as part of the AoA.

c. Provides recommendations to the Deputy Secretary of Defense for addressing, through the planning, programming, budgeting, and execution process, critical IT interoperability issues with affected DoD Components.

8. DOT&E. In addition to the responsibilities in section 12 of this enclosure, the DOT&E:

a. Requires that the NR KPP be addressed in operational tests and is an integral part of the evaluation of the system's operational effectiveness.

b. Requires that 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. Requires, with the DoD Business, Warfighting, Intelligence, and Enterprise Information Environment Mission Area Owners (DCMO, JCS, OUSD(I), and DoD CIO) and the other DoD Component heads, that capability-focused, architecture-based measures of performance and associated metrics are developed to support evaluations of IT interoperability throughout a system's life cycle.

d. Assists USD(AT&L) develop and maintain proper tools and testing infrastructure (to include a distributed operationally representative joint test environment) to support the development and evaluation of interoperable IT.

e. Assists the DoD Components with operational test planning and assessment or evaluation of the impact of IT interoperability on operational effectiveness, suitability, and survivability.

f. Includes interoperability in the OT&E final reports' evaluation of operational effectiveness, based primarily upon end-to-end testing within an operationally representative environment.

g. Requires that TEMPs (or equivalent documents) and operational test plans for those programs under DOT&E oversight identify IT interoperability test requirements with the USD(AT&L) and the other DoD Component heads. Emphasizes evaluation of IT interoperability as early as possible during a system's development.

h. Sponsors and manages joint test and evaluations to identify IT interoperability shortfalls and issues, in coordination with the DoD Components.

i. Requires and verifies, in coordination with CCMDs and Military Services, that respective subordinate organizations schedule at least one major exercise every year with interoperability as a major objective of the exercise.

j. Co-chairs the ITEP with the USD(AT&L) and DASD(DT&E). For details on ITEP functions, see section 8 of Enclosure 3 of this instruction.

9. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I), and in addition to the responsibilities in section 12 of this enclosure, the Director, DIA:

a. Collaborates with the DoD Components, as appropriate, to improve IT interoperability and to identify required interfaces between DIA IT and other DoD Component systems.

b. Coordinates with the DoD Components to satisfy IT interoperability requirements for processing intelligence and counterintelligence information.

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

d. Coordinates with the DoD Components to resolve IT interoperability issues. If resolution cannot be achieved, provide an impact statement and recommendations for resolution to the ISG.

10. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS). Under the authority, direction, and control of the USD(I), and in addition to the responsibilities in section 12 of this enclosure, the DIRNSA/CHCSS:

a. Serves as the DoD lead for approving and enforcing signals intelligence (SIGINT) architectures, in coordination with the DoD Components.

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

c. Requires interoperability and security of NSA/CSS IT with those systems that provide direct support to the Combatant Commanders.

d. In cooperation with the other DoD Components, satisfies 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.

e. In cooperation with other appropriate DoD Components, the IC, or other U.S. Government agencies, satisfies NSA/CSS IT interoperability requirements for processing foreign intelligence and foreign counterintelligence information by designing and developing interoperable and supportable technical, procedural, and operational interfaces.

f. Coordinates with the DoD Components to resolve IT interoperability issues. If resolution cannot be achieved, provide an impact statement and recommendations for resolution to the ISG.

g. Manages the interoperability requirements for cybersecurity (formerly IA)-enabled IT products for NSS in accordance with Committee on National Security Systems Policy No. 15 (Reference (r)).

11. DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA). Under the authority, direction, and control of the USD(I), and in addition to the responsibilities in section 12 of this enclosure, the Director, NGA:

a. Serves as the DoD Lead for GEOINT standards. Prescribes, mandates, and enforces standards and architectures related to GEOINT and confirms the integration of GEOINT standards and architectures in DoD GEOINT and GEOINT-related systems.

(1) Takes part in reviews of all GEOINT-related ISPs.

(2) Takes part in the review of all GEOINT-related requirements to verify the NR KPP is adequately defined for GEOINT.

(3) Coordinates with interoperability certification authorities to ensure that GEOINT-related interoperability test and evaluation criteria, measures, and requirements are fulfilled before those authorities grant 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 ~~DoDD~~ *DoD Instruction* 8320.02 (Reference (s)).

c. Coordinates with the DoD Components to resolve IT interoperability issues. If resolution cannot be achieved, provide an impact statement and recommendations for resolution to the ISG.

12. OSD AND DoD COMPONENT HEADS. The OSD and DoD Component heads:

a. Oversee implementation of the responsibilities and procedures in this instruction, including:

(1) Development and certification of the NR KPP for DoD Component IT.

(2) Development, review, and approval of DoD Component IT ISPs.

(3) Interoperability test, evaluation, and certification of IT before connection to a DoD network.

b. Establish procedures consistent with this instruction for interoperability certification for IT that does not have joint, multinational, or interagency interoperability requirements.

c. Establish procedures consistent with this instruction for reviewing DoD Component IT, determining when interoperability functionality or requirements have changed, and requiring the PM to submit that IT for interoperability recertification in accordance with Enclosure 3 of this instruction.

d. Designate representatives to fill the critical roles specified in Enclosure 3 of this instruction, including:

(1) System sponsors to execute the roles and responsibilities specified in Enclosure 3.

(2) An NR KPP Certification Authority for all IT that are not governed by Reference (h), that the CJCS has determined have no joint, multinational, or interagency interoperability requirements, as described in Enclosure 3, and have been delegated to the DoD Component by the CJCS for NR KPP certification.

(3) An Interoperability Certification Authority for all DoD Component IT with no joint, multinational, or interagency interoperability requirements and not governed by Reference (h), as described in Enclosure 3.

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

f. Design, develop, test, evaluate, and incorporate IT interoperability into all DoD Component IT.

(1) Require that interoperability requirements are coordinated with the CJCS and the Combatant Commanders, and that each IT system design identifies all external IT interfaces with required joint, multinational, interagency, and other non-DoD systems.

(2) Recommend tradeoffs among operational effectiveness, operational suitability, cybersecurity (formerly IA), survivability, and IT interoperability to the USD(AT&L), the DoD CIO, and the CJCS.

(3) Require IT programs be adequately funded to execute the interoperability functions specified in this instruction.

g. Require that all initial architectural views submitted either as part of an ISP, enterprise architecture, reference architecture, or solution or other architecture be in accordance with the current version of the DoD Architecture Framework (DoDAF) (Reference (t)). However, PMs may submit subsequent views (representing the same version of the system) either in accordance

with the original DoDAF version used, or the most current version. PMs will not be required to update architectural views solely to comply with changes in the DoDAF.

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

i. Require the DoD Component CIO to:

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

(2) Oversee the development, use, and maintenance of the DoD Component architectures (enterprise, reference, and solution) that are consistent with the latest version of the DoD Information EA (Reference (u)), and support development of ISPs and the architecture data recommended in this instruction.

(3) Advise the DoD Component head of alternatives and solutions to identified interoperability issues.

(4) Develop guidance to require and verify that DoD Component IT is interoperable and supportable with other relevant IT internal and external to the DoD Component.

(5) Take part in ISP reviews other DoD Components conduct.

13. CJCS. In addition to the responsibilities in section 12 of this enclosure, the CJCS:

a. Provides specific guidance on preparation, format, content, timelines for submission, and review of the NR KPP.

b. Establishes policy and procedures for developing, coordinating, and certifying the NR KPP, in coordination with the USD(AT&L), the DOT&E, and the other DoD Component heads.

c. Serves as the NR KPP Certification Authority, as described in Enclosure 3 of this instruction, for all IT with joint, multinational, or interagency interoperability requirements. Determines which IT has such requirements through the JCIDS and ISP review processes, and may either certify other IT without such requirements or delegate that IT to the appropriate DoD Component for NR KPP certification.

d. Requires and verifies, in coordination with the USD(AT&L), the DoD CIO, and the other DoD Components, that the content of joint operational concepts, and associated doctrine and operational procedures, address interoperability of IT used by 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 DoD Components for IT interoperability matters.

f. Establishes processes and procedures, in coordination with the DoD CIO, the USD(AT&L), the DOT&E, and the other DoD Component heads, to present insights gained from joint, multinational, and interagency operations, exercises, assessments, and experiments on IT interoperability to the USD(AT&L), the DoD CIO, the DOT&E, and the ISG.

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

h. Designates a representative to serve as ISG tri-chair together with DoD CIO and USD(AT&L) representatives. For details on ISG structure and functions, see section 8 of Enclosure 3 of this instruction.

i. Assesses interoperability in support of the ISG reviews.

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

14. COMBATANT COMMANDERS. In addition to the responsibilities in section 12 of this enclosure, Combatant Commanders may establish additional interoperability criteria beyond those found in this instruction, if required to meet operational needs. Coordinate additional CCMD interoperability criteria with OSD, CJCS, and DoD Components and integrated into DoD roadmaps in emerging and fielded systems.

15. COMMANDER, U.S. STRATEGIC COMMAND (CDRUSSTRATCOM). In addition to the responsibilities in sections 12 and 14 of this enclosure, the CDRUSSTRATCOM:

a. Serves as the chief advocate for CCMDs on tactical communications interoperability.

b. Assesses IT interoperability from the warfighter's perspective.

c. Requires that joint tactical network architectures are defined, developed, integrated, coordinated, validated, and synchronized with the Joint On-Demand Interoperability Network Lab (Reference (v)) (basis for the Joint Users Interoperability Communications Exercise and the DoD Interoperability Communications Exercise networks) and JITC (basis for interoperability certification and assessments) for the CCMDs.

d. Reviews and comments on the sufficiency of the NR KPP.

e. Requires that CCMD tactical systems, within a given capability, address interoperability from initial requirements development and throughout the system's life cycle.

f. Solicits, from the other Combatant Commanders, joint, multinational, and interagency IT interoperability issues, and presents to the ISG as required.

g. Identifies, consolidates, and prioritizes IT interoperability issues affecting emerging and fielded systems in coordination with the other Combatant Commanders.

h. Serves as the CCMD sponsor for all joint communications interoperability exercises.

i. Issues supporting warning and tactical directives and orders.

j. Directs corrective actions of any DoD Component enclave or IT on the enclave not in compliance with this instruction.

# ENCLOSURE 3

# PROCEDURES

1. GENERAL. The processes and procedures described in this enclosure provide the means by which the DoD CIO accomplishes oversight to the interoperability of IT. For each IT in development, measurable interoperability requirements must be identified, formally validated through NR KPP certification, and then formally tested through an interoperability certification process.

a. This enclosure primarily focuses on IT with joint, multinational, and interagency interoperability requirements. Such IT is within the purview of the CJCS for NR KPP certification, and JITC commander for interoperability certification.

b. Each DoD Component will certify the NR KPP for IT not having joint, multinational, or interagency interoperability requirements if authorized by the CJCS. Each DoD Component will conduct interoperability certification for IT not having joint, multinational, or interagency interoperability requirements as determined by the CJCS. The DoD Components will establish test and certification procedures for this IT based on the procedures defined in this enclosure.

## 2. INTEROPERABILITY REQUIREMENTS IDENTIFICATION

a. DoD Components and PMs will identify interoperability requirements through:

(1) The JCIDS and DOTMLPF-P change recommendation processes, as outlined in CJCS Instruction (CJCSI) 3170.01H (Reference (w)).

(2) The Defense Acquisition System, as defined in References (p) and (q), including the BEA and the BCL for defense business systems.

(3) Compliance and alignment with requirements from the applicable portions of the DoD EA (as defined in Reference (b)), consisting of mission area architectures (warfighting, business, intelligence, and enterprise information environment); applicable laws, regulations, policies, and guidance; DoD-wide reference and solution architectures; and DoD Component architectures. Key interoperability portions of the DoD EA include:

(a) The business rules of Reference (u).

(b) IT standards as specified in the DoD IT Standards Registry (DISR) (Reference (x)).

(c) Cybersecurity (formerly IA) requirements of References (l), (m), and (r).

(d) Data sharing requirements and use of the Data Services Environment as specified in Reference (s) and ~~DoD 8320.02-G~~ *DoD Instruction 8320.07* (Reference (y)).

(e) Spectrum use and electromagnetic spectrum data sharing requirements as specified in DoDI 4650.01 (Reference (z)) and DoDI 8320.05 (Reference (aa)).

(f) Network, information exchanges, and technical standard requirements described in applicable peer solution architectures and governing reference architectures. These interoperability requirements are derived from system resource flows and applicable technical standards as defined in the Reference (t).

b. Interoperability requirements must be documented in a succinct, measurable, and testable manner as an NR KPP. The NR KPP must describe a set of performance measures (MOEs and MOPs). The NR KPP must assess 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.

(1) The CJCS provides specific guidance on the preparation, format, content, and timelines for submission, review, and certification of the NR KPP.

(2) The NR KPP must be specified and included in either JCIDS requirements documents or an information support plan (ISP) (for those systems not covered by JCIDS), and must be updated throughout the IT life cycle when changes affect interoperability.

(3) Any system that connects to DoD networks must meet the threshold requirements of the NR KPP before connection.

(4) The NR KPP must document specific interoperability performance measures to guide system design and development.

(5) The NR KPP must be used by the DoD Component Lead DT&E Organization, DoD Component Operational Test Agency (OTA), or JITC as the basis to define test criteria to evaluate the interoperability of a given solution set. The NR KPP should be certified early so that it can be used during all test phases.

(6) DoD Components must submit the NR KPP for certification throughout a system's life cycle as the CJCS directs.

3. NR KPP CERTIFICATION PROCESS. NR KPP certification ensures the NR KPP is correct and sufficient in scope and content to describe a system's interoperability requirements in a measurable and testable manner that meets DoD interoperability needs. NR KPP certification for all IT, both ACAT and non-ACAT, must occur before interoperability test and evaluation, leading to interoperability certification.

a. PMs must document and submit NR KPPs for certification in accordance with Reference (w) and CJCSI 6212.01F (Reference (ab)) for all ACAT, non-ACAT, and fielded IT acquisitions and procurements. DoD Components will certify NR KPPs for IT without joint, multinational, or interagency interoperability requirements when authorized by CJCS.

b. The NR KPP Certification Authority will record the results of NR KPP certification in the authoritative IT registry.

c. Upon significant upgrade to the system affecting interoperability or before requesting interoperability recertification (in accordance with section 6 of this enclosure), PMs will submit the NR KPP for recertification by the NR KPP Certification Authority in accordance with References (a) and (ab). This ensures that the interoperability requirements remain synchronized with current and planned operational contexts.

## 4. ISP PROCESS

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

(1) The PM must use the ISP as a tool to identify and resolve risks and issues related to a program's IT information infrastructure support and information interface requirements. The PM uses the ISP as a key input to a system's TEMP.

(2) The DoD CIO and the DoD 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.

(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 production or deployment representative 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 ISP, the PM must submit architectural views (listed in the IPG) to describe the interoperability requirements of the IT. The ISP review process will assist the PM to refine these views, and result in a set of detailed measurable interoperability criteria for use in interoperability test and certification.

b. Development and Submission

(1) PMs must develop the ISP online by entering system information through the GTG-F portal (https://gtg.csd.disa.mil). ISP formatting and content requirements are specified by the

GTG-F and described in the Defense Acquisition Guidebook (DAG) (Reference (ac)). Deviations from these requirements require the DoD Component's approval. Until GTG-F is available on the Secret Internet Protocol Router Network, Secret ISPs are submitted and approved using the DISA Interoperability and Supportability Legacy Data Repository. 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 and the points of contact. Classified ISPs use the format and content requirements described in the DAG until the GTG-F is available on the appropriately classified network.

(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 minimized in the ISP.

(3) PMs of ACAT II and below programs and non-ACAT systems may tailor the ISP to the system's scale, complexity, and available resources with the approval of the DoD Component head.

(a) DoD Components may only approve a tailored ISP using these criteria: legacy programs in sustainment with no plan of upgrade, non-ACAT programs with limited resources, or programs with a scheduled date of retirement in the near future.

(b) At a minimum, the tailored plan provides an explanation of the program's concept of operations (CONOPS) and provides IT supportability analysis of the CONOPS.

(c) For IT with joint, multinational, or interagency interoperability requirements, tailoring of the required architecture views in the ISP (as specified in the IPG) require CJCS, DoD Component, and JITC concurrence.

(d) The final DoD Component tailored ISP is submitted to the GTG-F for review and approval.

(4) PMs must submit the NR KPP and required architectural data in the ISP to support interoperability test and certification. The ISP must include existing KPP(s) or key system attributes that specifically describe required information exchanges. For IT whose requirements are governed by References (p) or (w), the official version of the NR KPP is found in the approved requirements document. The ISP must contain, provide a link to, or duplicate the appropriate section of the requirements document. For all other IT, the ISP must contain the official NR KPP, along with proof of NR KPP certification, when received.

(5) PMs must submit ISPs for review at multiple milestones or key decision points during a program's life cycle as described in Reference (q). The DoD Component must approve the ISP before each milestone or key decision point where the ISP is required.

(a) PMs submit the ISP a minimum of 60 days before the milestone or decision point, to allow for a 30-day review period and a 30-day comment adjudication period.

(b) A PM may coordinate a longer adjudication period with the milestone decision authority (MDA) or other decision maker if the comments received warrant more time for adjudication. Systems fielded in increments follow the entire ISP submission and review process for each increment.

(c) For IT programs governed by Reference (p):

1. ISP submissions are linked to various milestones (e.g., B, and C) and review points within the Defense Acquisition Management System, as described in Reference (q).

2. The PM submits an initial ISP before, and in support of, the pre-engineering and manufacturing development (EMD) review before milestone B. The initial ISP should aid in the development of the EMD phase request for proposal.

3. The PM submits the revised ISP before the critical design review (CDR). PMs of programs with multiple CDRs must coordinate this submission with the DoD Component ISP point of contact and DoD CIO as appropriate. The revised ISP may be waived or become the ISP of record based on DoD Component approval.

4. The PM submits the ISP of record before milestone C, unless the DoD Component determines otherwise. The DoD Component provides final approval of the ISP of record. The ISP of record must describe the production or deployment representative system.

5. The PM submits an updated ISP for single milestone program upgrades during life-cycle sustainment, as required. Once the DoD Component approves, this updated ISP becomes the ISP of record. An update to the ISP may be required to support interoperability test and certification for a given increment or upgrade of the system architecture.

(d) For IT programs not governed by Reference (p), the owning DoD Component must institute equivalent milestone events in the program's development to the Defense Acquisition System process, and conduct ISP submissions and reviews accordingly.

(e) For all IT programs:

1. The DoD Component must approve an updated ISP before fielding a new program increment or update.

2. The PMs of IT programs that do not receive NR KPP certification via the JCIDS process must submit the ISP at least 60 days before the scheduled submission date to the NR KPP Certification Authority, to allow 30 days to review and 30 days to adjudicate comments.

c. ISP Review and Approval

(1) During a review, the owning DoD Component must staff the ISP to the appropriate entities for comment using the GTG-F, then work with the PM to adjudicate the comments. The

PM adjudicates critical comments by actively engaging with the organization and person who made the comment. The DoD Component must review and approve the ISP each time it is submitted.

(2) DoD Components must establish processes to conduct reviews of unclassified ISPs within the GTG-F (https://gtg.csd.disa.mil). DoD Components should conduct concurrent joint and internal DoD Component reviews as often as possible. DoD Components that do not have a mature ISP review process may request DoD CIO assistance with conducting joint reviews.

(3) The DoD Component must lead the review of all ISPs, regardless of ACAT level. If a program meets the criteria for a joint review listed below, the DoD Component must staff the ISP for review:

(a) For ACAT II and below IT programs, as well as non-ACAT, the owning DoD Component must select the appropriate additional DoD Components to participate for the joint review; however, the review must include, at a minimum, the Joint Staff, DISA, and the DoD Components specified in the joint, multinational, and interagency requirements of that IT.

(b) For all ACAT I IT programs, the owning DoD Component must staff the ISP to all DoD Components as part of a DoD-level joint review.

(c) The DoD CIO may declare any ISP to be of special interest. The DoD Component must include the DoD CIO on all reviews of ISPs declared as DoD CIO "special interest." As part of its review, the DoD CIO must provide concurrence, concurrence with comment, or non-concurrence with the ISP for the DoD Component, MDA, or relevant fielding authority's consideration for final approval.

(d) DoD Components conduct joint reviews for all IT that:

1. Have joint, multinational, or interagency interoperability requirements.

2. Have a Joint Staffing Designator (formerly Joint Potential Designator) of Joint Requirements Oversight Council interest, Joint Capabilities Board interest, or Joint Integration.

3. Received a DoD Component determination that a joint review is necessary.

(e) DoD Components must include NGA in the review of all ISPs for GEOINT-related IT.

(4) For critical comments that cannot be resolved, the issue is elevated through the owning DoD Component head's designated representative for the DoD CIO's resolution. The PM must brief critical risks and issues identified through ISP reviews to Integrated Product Teams, as appropriate.

(5) All critical comments must be fully adjudicated before issuing the final approval of the ISP of record.

(6) All ISP reviews, joint or internal, must include the CJCS for certification of the NR-KPP (or for NR KPP review of IT having already received NR KPP certification through the JCIDS process or DoD Component process).

## 5. IT INTEROPERABILITY TEST AND EVALUATION

a. NR KPP Certification Authorities will certify the NR KPP according to section 3 of this enclosure before testing for interoperability certification or recertification.

b. For IT developed in accordance with Reference (q), the DT authority for that IT should provide the MDA at Milestone C, an assessment of DT&E which must include a verification that all interoperability related DT has been completed and that 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. Copies of those assessments should be provided to the DASD(DT&E) and the appropriate Chief DT&E authority within the DoD Component.

c. For IT with joint, multinational, and interagency interoperability requirements:

(1) The JITC commander or designated representative must:

(a) Review and comment on the interoperability test and evaluation strategy included in the TEMP and on detailed test and evaluation plans for interoperability events.

(b) Review and provide coordinating comments on TEMPs or equivalent documents, and provide, to the DT&E approval authority, an assessment of interoperability testing adequacy.

(c) Take part in the system's Test and Evaluation Working Integrated Process Team or equivalent.

(d) Recommend IT interoperability test and evaluation criteria for test plans.

(2) PMs 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 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.

d. For IT without joint, multinational, or interagency interoperability requirements, the DoD Component will conduct all interoperability test and evaluation.

e. DoD Components should leverage test and evaluation capability and activities that support interoperability testing across the DoD. DISA must use a distributed test capability to keep pace with emerging technology and the large demand from the DoD Components for interoperable

and secure IT. DoD Components should incorporate DoD Component test labs in the test and certification processes to allow more timely delivery of emerging technologies to the warfighter and business communities. Under this concept:

(1) The DoD Component labs may be used for interoperability test and evaluation for ACAT II and below, non-ACAT, and fielded systems.

(2) For IT with joint, multinational, or interagency interoperability requirement, the DoD Components must provide the results of interoperability testing to JITC for evaluation, in a JITC-prescribed format. JITC must oversee the interoperability test and evaluation process the DoD Components conduct to ensure there is adequate data for interoperability certification.

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

g. Interoperability testing must replicate the system's operational network environment to the maximum extent possible, including the cyber threat environment.

h. The DoD Component Chief Developmental Tester and Lead Developmental Test and Evaluation Organization must include evaluation criteria in IT interoperability test event plans.

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

j. DoD Component heads must:

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

(2) Require all test plans be sufficient to verify that the system meets the NR KPP requirements.

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

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

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

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

(7) Provide the DoD Component's portion of the test and evaluation infrastructure.

## 6. IT INTEROPERABILITY CERTIFICATION PROCESS

a. Overview. Interoperability Certification Authorities will verify a system's compliance with the NR KPP requirements (MOEs and MOPs) through test and evaluation. If the system meets the threshold values of the NR KPP, Interoperability Certification Authorities will certify the system for interoperability.

(1) NR KPP Certification Authorities must certify the NR KPP before testing for interoperability certification and any recertification.

(2) PMs must achieve interoperability certification (or obtain an ICTO) for IT systems before a DoD network connection approval decision (approval to connect (ATC) or interim approval to connect (IATC)).

(3) PMs must submit system(s) for recertification when interoperability functionality or requirements changes, as determined by the owning DoD Component. Otherwise, PMs of systems with joint, multinational, or interagency interoperability requirements must report to the ISG every 4 years to determine if recertification is required, or if the existing certification will be extended for an additional 4 years. Where there is disagreement whether a recertification is required, it will be brought before the ISG for resolution.

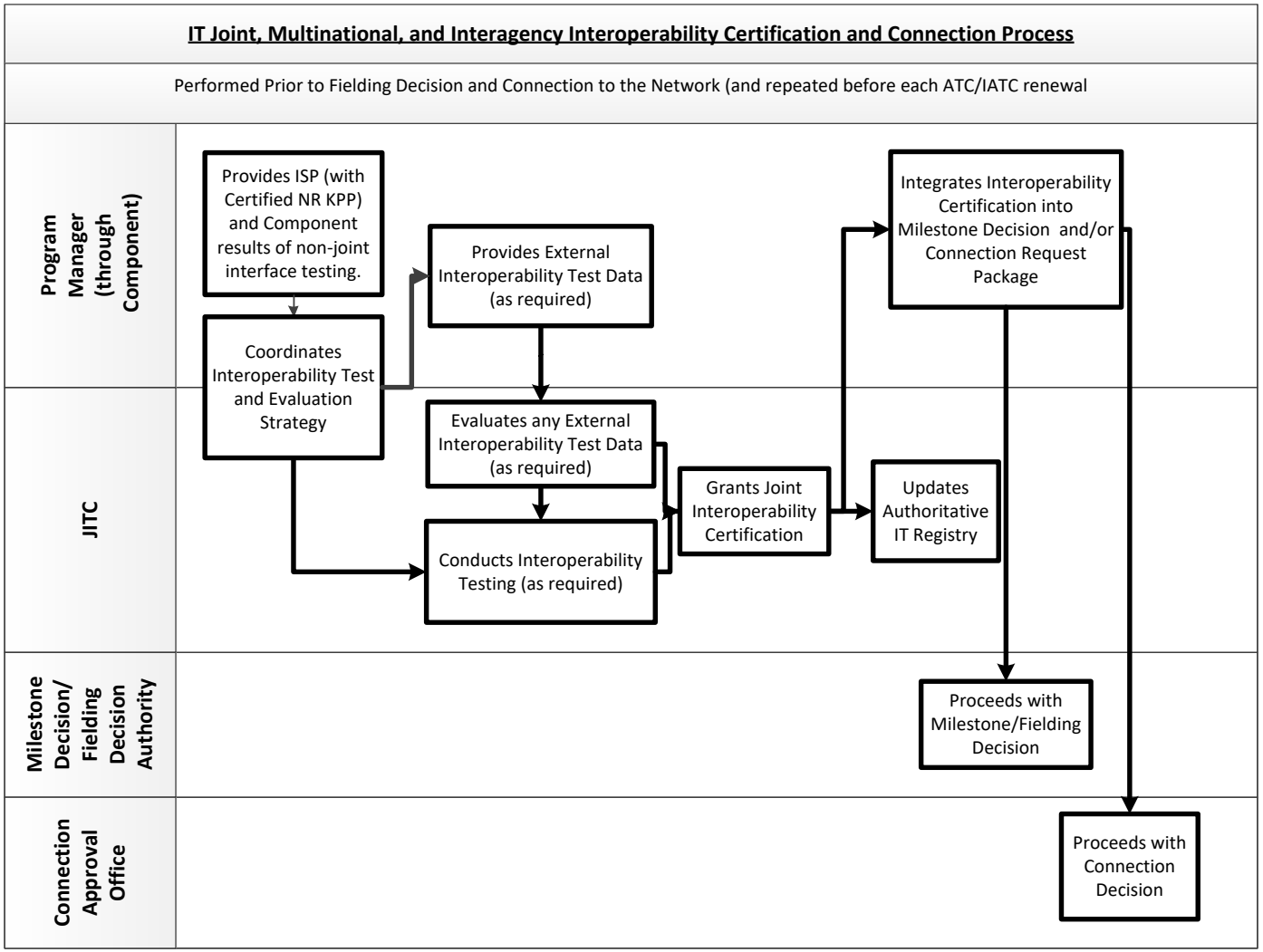
(4) The Figure on the next page depicts the interoperability certification and connection process for IT with joint, multinational, and interagency interoperability requirements.

(5) JITC serves as the Joint Interoperability Certification Authority, under the oversight and direction of the DoD CIO, for IT with joint, multinational, and interagency interoperability requirements. Each DoD Component head must establish an Interoperability Certification Authority for IT systems that have no joint, multinational, or interagency interoperability requirements.

b. Procedures

(1) Interoperability must be assessed for certification through formal developmental and operational test and evaluation by DoD Component developmental test agencies, OTA, JITC, joint exercises, other formal assessments, or a combination of any of these. The Interoperability Certification Authority determines whether adequate test and evaluation has been performed before interoperability certification.

Figure. IT Interoperability Certification and Connection Process For Systems with Joint, Multinational, or Interagency Interoperability Requirements



(a) JITC serves as the Joint Interoperability Certification Authority for the DoD. As such, JITC must develop procedures to verify, assess, and certify, through testing (or review of other organizations' testing), the interoperability of IT (ACAT and non-ACAT).

(b) JITC will develop and publish an online IPG, in coordination with the DoD CIO, to document procedures and data requirements for interoperability testing and certification, waiver processing, and associated processes and procedures. The IPG will be available at http://jitc.fhu.disa.mil/cgi/icpsite/pubs.aspx.

(2) PMs, via their DoD Component, must provide the appropriate Interoperability Certification Authority with the proposed interoperability test and evaluation strategy (from the TEMP) and the ISP of Record. If the Interoperability Certification Authority is JITC, the DoD Component must also provide confirmation that the system has been tested and has met all its joint, multinational, and interagency interoperability requirements.

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

(4) Upon completion of interoperability test and evaluation, the Interoperability Certification Authority must make the interoperability certification decision and notify the DoD Component, PM, and sponsor. If the Interoperability Certification Authority decides not to certify, then the Interoperability Certification Authority must identify those NR KPP attributes, threshold measures, or objective measures that were not met, and the impact those missed thresholds would have on the operation of the system and completion of the mission. The Interoperability Certification Authority records the results of the certification decision in the authoritative IT registry, 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 (ATC or IATC).

(5) An interoperability certification may list operational restrictions. For example, if a particular interface could not be successfully tested, the system may, at the discretion of the Interoperability Certification Authority, receive certification that allows the system to operate, but restricts it from using the interface in question. A PM wishing to begin using that interface must submit the system for additional interoperability testing in order to have the restriction removed.

c. Certification of Urgent and Emergent Operational Need-Based IT. IT initiated through a validated urgent operational need (UON) or emergent operational need, as defined in Reference (w), does not require an ISP or Joint, Multinational, and Interagency Interoperability Certification before network connection, unless the capability meets the threshold for a Major Defense Acquisition Program or Major Automated Information System. The DoD Component must place IT using this exemption on the OARL before network connection.

(1) Subject to any DoD CIO and DoD Component guidance, individual enclave owners must determine whether to allow IT listed on the OARL to connect. Enclave owners may require some additional level of interoperability evaluation for risk mitigation purposes.

(2) If IT fielded under the authority of an urgent or emergent operational needs document continues to operate after the expiration of that document, it must undergo interoperability certification in accordance with this instruction.

d. Recertification

(1) PMs must submit their IT systems for recertification when interoperability functionality or requirements change, as determined by the owning DoD Component.

(2) Otherwise, PMs will report to the ISG (or equivalent DoD Component governing body for systems without joint, multinational or interagency interoperability requirements) every four years to determine if recertification is required or if the existing certification will be extended for an additional four years.

(3) The IPG will provide specific procedures for interoperability recertification.

## 7. SYSTEM CONNECTION APPROVAL

a. Once a system has completed interoperability certification, the PM is authorized to apply for network connection through the appropriate enclave or network owner. The enclave or network owner must not connect the system without a valid interoperability certification, ICTO, or valid waiver. If none of these conditions are met, the enclave or network owner must refer the PM to the ISG, via the PM's DoD Component ISG representative, for resolution before connection.

b. DoD Component heads must oversee this process for connecting IT systems to enclaves owned by the DoD Component and provide appropriate guidance and procedures for PMs to follow.

c. The DISA CAO must not issue or renew an ATC or IATC 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 DoD Component 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 that have not completed interoperability certification and could pose an interoperability risk to other systems on the network. DISA updates and distributes the OARL at least quarterly to all DoD MDAs; affected system fielding authorities (for non-ACAT IT); the CJCS; the DoD Component CIOs;

the Commander, USSTRATCOM; and the DISA CAO. The USD(AT&L) and DoD Component heads assist DISA to distribute the OARL to all DoD Component MDAs and affected systems fielding authorities.

## 8. INTEROPERABILITY GOVERNANCE

a. The ISG will be subordinated to an appropriate forum of the DoD CIO EB, as determined by the DoD CIO. The ISG proposes, reviews, and coordinates interoperability policies; reviews critical interoperability issues; and adjudicates requests for ICTOs, waivers to policy and renewal of interoperability certifications. Representatives from the DoD CIO, the USD(AT&L), and the CJCS tri-chair the ISG. DoD Components will provide representatives to the ISG, as appropriate. The ISG Charter will be signed by general officer or senior executive service representatives of the DoD CIO, USD(AT&L) and CJCS, and then published by the DoD CIO. Representatives submit interoperability issues that cannot be resolved to ISG for resolution.

b. The ITEP is a separate entity, co-chaired by representatives from DASD(DT&E) and DOT&E, with membership representation from the DoD Components, as appropriate. The ITEP oversees and enforces a T&E process where interoperability requirements are measurable and testable; T&E is adequately planned, resourced, and coordinated; assessments address the impacts of interoperability on operational effectiveness; and performance of fielded systems is watched. Semiannually, a summary of the ITEP's activities and findings must be provided to the DoD CIO EB.

## 9. WAIVERS TO IT INTEROPERABILITY POLICY AND ICTO REQUESTS

a. DoD Component heads may approve requests to waive the requirement for an ISP, interoperability testing, or interoperability certification for DoD Component-unique (i.e., no joint, multinational, or interagency interoperability requirements) IT. Upon approval, the DoD Component provides the DoD CIO with copies of the waiver request and approval memorandums.

b. Only the DoD CIO, in coordination with the USD(AT&L), DOT&E, the NGA and the DoD mission area owners (OUSD(I), DCMO, and CJCS), as appropriate, is authorized to approve any other waivers to this instruction. The DoD CIO, in coordination with the USD(AT&L), the DOT&E, and the CJCS, will consider waivers to this instruction only:

(1) When the operational chain of command and the 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 OSD or DoD Component head concerned.

(3) When the requesting DoD Component can demonstrate that the cost of complying with this policy outweighs the benefit to the DoD.

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

d. The DoD CIO, in coordination with the USD(AT&L) and the CJCS, grants ICTOs for systems with joint, multinational, and interagency interoperability requirements. The DoD Component heads grant ICTOs for all other systems. ICTOs must only be granted when the system is undergoing interoperability certification testing and there is a documented need to operate the system before completing interoperability test and certification.

e. Submit waivers and requests for ICTOs in accordance with the IPG.

f. JITC must review all requests for waivers of interoperability policy requiring DoD CIO approval, analyzes those requests, and provides a recommendation to the DoD CIO within 15 calendar days of the waiver request.

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

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

# GLOSSARY

## PART I. ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| ACAT | acquisition category |
| AoA | analysis of alternatives |
| AoR | area of responsibility |
| ASD(HD&~~ ASA~~*GS*) | Assistant Secretary of Defense for Homeland Defense and ~~Americas' Security Affairs~~ *Global Security* |
| ATC | approval to connect |
| | |
| BCL | Business Capability Lifecycle |
| BEA | Business Enterprise Architecture |
| | |
| CAO | Connection Approval Office |
| CCMD | Combatant Command |
| CDR | critical design review |
| CDRUSSTRATCOM | Commander, U.S. Strategic Command |
| CIO | Chief Information Officer |
| CJCS | Chairman of the Joint Chiefs of Staff |
| CJCSI | Chairman of the Joint Chiefs of Staff Instruction |
| CNSS | Committee on National Security Systems |
| CONOPS | concept of operations |
| | |
| DAG | Defense Acquisition Guidebook |
| DASD(DT&E) | Deputy Assistant Secretary of Defense for Developmental Test and Evaluation |
| DCAPE | Director of Cost Assessment and Program Evaluation |
| DCMO | Deputy Chief Management Officer |
| DIA | Defense Intelligence Agency |
| DIRNSA/CHCSS | Director, National Security Agency/Chief, Central Security Service |
| DISA | Defense Information Systems Agency |
| DISN | Defense Information Systems Network |
| DISR | DoD IT Standards Registry |
| DNI | Director of National Intelligence |
| DoD CIO | DoD Chief Information Officer |
| DoD EA | DoD Enterprise Architecture |
| DoDAF | DoD Architecture Framework |
| DoDD | DoD Directive |
| 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 | developmental testing |

| | |
|---|---|
| DT&E | developmental test and evaluation |
| EB | Executive Board |
| EMD | engineering and manufacturing development |
| GEOINT | geospatial intelligence |
| GTG-F | Global Information Grid Technical Guidance Federation |
| IA | information assurance |
| IATC | interim approval to connect |
| IC | Intelligence Community |
| ICTO | interim certificate to operate |
| IPG | Interoperability Process Guide |
| ISG | Interoperability Steering Group |
| ISP | information support plan |
| IT | information technology |
| ITEP | Interoperability Test and Evaluation Panel |
| JCIDS | Joint Capabilities Integration and Development System |
| JITC | Joint Interoperability Test Command |
| MDA | milestone decision authority |
| MOE | measure of effectiveness |
| MOP | measure of performance |
| NGA | National Geospatial-Intelligence Agency |
| NR KPP | net ready key performance parameter |
| NSA | National Security Agency |
| NSS | National Security Systems |
| OARL | Operating at Risk List |
| OT&E | operational test and evaluation |
| OTA | operational test agency |
| OUSD(I) | Office of the Under Secretary of Defense for Intelligence |
| PM | program manager |
| SIGINT | signals intelligence |
| TEMP | Test and Evaluation Master Plan |
| UC | unified capabilities |
| UON | urgent operational need |
| USD(AT&L) | Under Secretary of Defense for Acquisition, Technology, and Logistics |
| USD(C)/CFO | Under Secretary of Defense (Comptroller)/ Chief Financial Officer, Department of Defense |

USD(I) Under Secretary of Defense for Intelligence

## PART II. DEFINITIONS

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

ACAT. 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. Reference (q) provides the specific definition for each ACAT level.

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.

BCL. A holistic approach that emphasizes rigorous analysis of requirements to enable rapid delivery of business capabilities to the warfighter in a compressed timeframe. BCL aligns the existing DoD business capability policies by consolidating requirements, acquisition, and BEA compliance into a single oversight structure.

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 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.

cybersecurity. Defined in Reference (l).

defense business system. An information system, other than a national security system, operated by, for, or on behalf of the DoD, including financial systems, mixed systems, financial data feeder systems, and IT and cybersecurity (formerly IA) infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management.

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 (DISR elements), 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.

DT&E. A process that provides program managers 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.

EMD. Defined in Reference (q).

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.

enterprise architecture. The explicit description and documentation of the current and desired relationships among business and management processes and IT.

enterprise service. An enterprise service is any capability provided for broad use across the DoD that enables awareness of, access to, or delivers information across DoD networks.

Enterprise services may be provided by any source within the DoD or any trusted partners.

Enterprise services providing data or information must be authoritative and, therefore, trusted as being accurate, complete, and having assured integrity. Authoritative information has a pedigree that can be traced to a trusted source.

Enterprise services include environments that are composed of multiple service layers such as the infrastructure, infrastructure services, platform services, common user services, enterprise service management, and mission assurance services.

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. A portal to a set of online tools, run by DISA, which supports the verification of interoperability and supportability of systems on the Global Information Grid.

IA. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

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 interoperability certification. Issued by the ISG to PMs who have an urgent need to operate IT, have not completed interoperability certification, but are making satisfactory progress towards that goal (as determined by the ISG).

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. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with cybersecurity (formerly IA).

interoperability certification. A formal statement of adequacy, provided by the responsible interoperability certification authority agency, that a system has met its interoperability requirements.

Interoperability Certification Authority. The office with the certification authority for the interoperability. Verifies that the IT has met its interoperability requirements, as proven through

test and evaluation. For IT with joint, multinational, and interagency interoperability requirements, the Interoperability Certification Authority is JITC. For all other IT, the owning DoD Component designates the Interoperability Certification Authority.

interoperability requirements. A condition, situation, or capability in which interoperability deficiencies have been identified, based on an approved or established rule set, test, or measure of value for judging interoperability sufficiency of IT.

ISP. A set of information supporting interoperability test and certification. Entered through the GTG-F portal, the ISP contains or links to the NR KPP along with supporting architectural data. Instructions for completion of the ISP are found on the portal. The IPG and Reference (ac) provide additional information on the ISP.

IT. Defined in section 11101 of Title 40, United States Code (Reference (ad)).

IT architecture. Architecture of an enterprise's information technology (see architecture).

ITEP. A DoD forum focused on the continuum of developmental and operational T&E of interoperability from a DoD enterprise-wide perspective. Co-chaired by representatives from DASD(DT&E) and the DOT&E. 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 Reference (w).

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."

joint, multinational, or interagency interoperability requirement. Any requirement levied on an IT to implement information exchanges to other IT across or beyond a DoD Component's boundaries or implement a web service with the explicit or implicit intention to share information with other IT across or beyond a DoD Component's boundaries. Information exchanges and web services between the U.S. Navy and U.S. Marine Corps are considered joint.

KPPs. Minimum attributes or characteristics considered most essential for an effective military capability.

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 NR KPP 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. Current DoD acquisition milestones are defined in Reference (q).

mission area. Defined in Reference (g).

net ready. DoD IT that meets required information needs, information timeliness requirements, has a cybersecurity (formerly IA) 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. 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. 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. 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 (AOR).

Across CCMD AOR 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.

Across current and future systems.

NR KPP. The NR 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. The NR KPP consists of measurable and 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.

NR KPP certification. An authoritative act or process of supporting or corroborating whether IT interoperability requirements are appropriate and complete.

NR KPP Certification Authority. The office with the authority to certify the NR KPP. Verifies that the system sponsor has properly scoped, refined, and justified the interoperability requirements of the system. The CJCS is the NR KPP Certification Authority and may delegate this authority to the appropriate DoD Component for all IT with no joint, multinational, or interagency interoperability requirements.

NSS. Defined in section 3542(b) of Title 44, United States Code (Reference (ae)).

OTA. Organizations performing operational test and evaluation 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.

oversight. Senior executive-level review of programs to ensure compliance with policy and attainment of broad program goals.

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 signals intelligence.

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.

sponsor. The "customer" of the program manager. Advocate of the operational community who will use the system. Champions the systems requirements. Must have a scope of responsibility wide enough to be aware of the operational space the system will work within, and all the other systems, current and future, with which it should interoperate.

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 systems attainment of the technical performance, specifications, and system maturity.

UC. Defined in Reference (h).