DoD Instruction 8310.01

Information Technology Standards in the DoD

Originating Component:	Office of the DoD Chief Information Officer
Effective:	April 7, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 8310.01, "Information Technology Standards in the DoD," July 31, 2017, as amended
Approved by:	John B. Sherman, Chief Information Officer of the Department of Defense

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance establishes policy, assigns responsibilities, and authorizes a process for identifying, developing, adopting, establishing, prescribing, and publishing technical standards for DoD information technology (IT) in accordance with the guidance in DoDD 8000.01 and pursuant to Sections 142, 2223(a)(3), and 2224 of Title 10, United States Code (U.S.C.). These technical standards:

- Include national security systems (NSS) and defense business systems (DBS).
- Enable interoperability, information sharing, reuse, portability, innovation, and cybersecurity.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to:

(1) OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of 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 issuance as the "DoD Components").

(2) The Coast Guard will adhere to DoD cybersecurity requirements, standards, and policies in this issuance in accordance with the guidance in Paragraph 4a of the January 19, 2017 Memorandum of Agreement between the Department of Defense and the Department of Homeland Security.

(3) DoD IT, to include NSS and DBS or IT services that any DoD Component develops or procures, including:

(a) DoD IT that shares, exchanges, and uses DoD data and information.

(b) IT supporting business activities, including DBS, within the DoD.

(4) Mission partners by mutual agreements such as other departments and agencies of the U.S. Government, State and local governments, allies, coalition members, host nations, other nations, multinational organizations, non-governmental organizations, and the private sector.

b. This issuance does not apply to cleared contractors' information systems processing classified information under the National Industrial Security Program. Those systems are subject to certification and accreditation by the Defense Counterintelligence and Security Agency in its role as the Designated Approving Authority in accordance with DoD Instruction (DoDI) 5220.22.

c. This issuance does not alter or supersede existing authorities and policies of the Director of National Intelligence regarding:

(1) The protection of sensitive compartmented information and special access programs for intelligence pursuant to Executive Order 12333.

(2) National security information systems pursuant to Executive Orders 13231, 13587, and 14028; National Security Memorandum (NSM)-8; and other laws and regulations.

1.2. POLICY.

a. IT standards:

(1) Support the National Defense Strategy through the DoD Digital Modernization Strategy, DoD Software Modernization Strategy, DoD Data Strategy, the Modular Open Systems Approach, and Mission Partner Environment by enabling interoperability, information sharing, reuse, portability, cybersecurity, and innovation within the DoD and with mission partners.

(2) Support and comply with data, information, cybersecurity, physical, and operational security policy guidance.

(3) Support interoperability for physical access control in accordance with DoDI 5200.08.

b. Intra-agency and interagency support agreements established in accordance with DoDI 4000.19, and other necessary arrangements as required, may be used to fulfill assigned responsibilities, roles, and authorities delineated in this issuance.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO).

In addition to the responsibilities in Paragraph 2.9., the DoD CIO:

a. Serves as the OSD Principal Staff Assistant responsible for oversight and direction to establish, prescribe, and enforce IT standards that apply across the DoD.

b. Establishes, maintains, and enforces, in coordination with the DoD Component heads, the policy and processes for identifying, developing, adopting, prescribing, establishing, and publishing IT standards that apply throughout the DoD in accordance with:

(1) Sections 142 and 2223(a)(3) of Title 10, U.S.C.

(2) Public Law 108-237.

(3) Section 272 of Title 15, U.S.C.

(4) Office of Management and Budget (OMB) Circular A-119.

(5) OMB, United States Trade Representative, and Office of Science and Technology Policy Joint Memorandum M-12-08.

(6) OMB Circular A-130.

(7) DoDI 4000.19.

(8) DoDI 4120.24.

(9) DoDI 5000.75.

(10) DoDI 8320.07.

c. Designates a DoD representative to be the co-chair of the Joint Enterprise Standards Committee (JESC) and provides direction, oversight, and priorities for IT standards governance.

d. Coordinates with the Intelligence Community (IC) CIO and the Under Secretary of Defense for Intelligence and Security (USD(I&S)) to establish a community-based forum to develop policy and procedures for prescribing, establishing, and enforcing common IT standards, profiles, and other specifications for DoD and the IC in accordance with the Office of the Director of National Intelligence Chief Information Officer (ODNI/CIO) Memorandum ODNI/CIO-2009-165.

e. Provides oversight, with the DoD Components and the IC, for the development and maintenance of the DoD IT Standards Registry (DISR).

f. Coordinates with the Under Secretary of Defense for Research and Engineering (USD(R&E)), Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), USD(I&S), CJCS and the other DoD Component heads, and Component Acquisition Executives (CAEs) to:

(1) Ensure the use of, and compliance with, DoD IT standards mandated in DISR when developing or procuring IT capabilities.

(2) Ensure participation of subject matter experts in JESC and IT standards technical working group (TWG) activities.

g. Provides, in coordination with the DoD Component heads, annual direction and guidance to the Defense Information Systems Agency (DISA) on DoD IT standards objectives, priorities, and outcomes.

h. Coordinates DoD IT standards activities at the Federal Executive level.

i. Establishes processes and procedures for oversight, enforcement, and reporting of IT standards compliance in coordination with the USD(R&E); USD(A&S); Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense (USD(C)/CFO); USD(I&S); Director, DISA; CJCS; and other DoD Component heads, as required.

j. Approves the annual standards development organization (SDO) membership package submitted by DISA.

k. Validates the need for new IT standards in coordination with the Director, DISA; the USD(R&E); the USD(A&S); the CJCS; and other DoD Component heads.

l. Requires that funds and costs needed to support this issuance be identified and recommends that they be included in the IT budget.

m. Coordinates IT standards impacting the Business Mission Area through the Defense Business Council.

n. Approves DoD Component waiver requests to use an IT standard that is not registered in DISR as mandated or emerging. Paragraph 3.8. provides procedures for requesting a DoD IT standards compliance waiver.

o. Ensures that Digital Modernization Infrastructure Executive Committee-approved DoD Information Enterprise Architecture, including subordinate reference architectures and documents, comply with this issuance.

p. Requires that IT military standards (MIL-STDs) are published in ASSIST in accordance with DoDI 4120.24 and DoD Manual (DoDM) 4120.24 before adoption as described in Paragraph 3.4.

q. Endorses the DISR baseline memorandum in collaboration with the USD(A&S) and CJCS.

2.2. DIRECTOR, DISA.

Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in Paragraph 2.9., the Director, DISA:

a. Coordinates with the DoD Component heads, as appropriate, to identify and propose IT standards that support a capability-focused and architecture-based approach for achieving IT interoperability.

b. Develops and executes a clear IT standards management strategy to achieve interoperable IT.

c. Plans and executes DoD IT standards activities in coordination with the DoD Component heads and the IC.

d. Prepares and maintains, in coordination with DoD CIO and DoD Component heads, an annual SDO membership package. This package identifies the SDOs with which DoD needs to have membership and designates representatives to perform as the DoD representative to those organizations.

e. Articulates DoD IT standards requirements to influence and inform ongoing and future IT standards development by public and private IT sector SDOs.

f. Appoints the DoD representatives nominated by their Components to take part in external public and private sector IT standards forums and oversees DoD representation at multinational IT standards organizations.

(1) Collaborates with DoD Component heads to identify IT standards from authoritative sources for inclusion in the DISR such as voluntary consensus standards, Federal standards, IT MIL-STDs, and U.S.-ratified international standards agreements.

(2) Establishes and advocates DoD positions on IT standards issues in public and private sector IT standards forums.

(3) Supports the DoD CIO in execution of IT standards, guidance, direction, and oversight of IT standards activities at the Federal Executive level.

(4) Coordinates DoD adoption of and positions on IT standards with the National Institute of Standards and Technology (NIST) and other Federal agencies, as appropriate.

(5) Collaborates with military, Federal, national, and international standards bodies to identify emerging IT standards.

(6) Coordinates with national and international standards bodies and sets up the appropriate methods, profiles, and test suites for IT standards conformance.

(7) Provides to the JESC co-chairs 30 days before JESC Plenary meetings a status report about public and private IT standards working group activities, forums, and collaborative development efforts.

(8) Provides DoD Component heads and their IT staff with access to IT standards-related information that is included by the SDO membership privileges. This does not include payment of a license or separate royalty fee for use of the standard.

g. Influences commercial vendors to develop off-the-shelf products that satisfy DoD IT standards requirements in accordance with Federal policy and the U.S. Standards Strategy.

h. Coordinates with the DoD CIO; USD(R&E); USD(A&S); and the CJCS; and other DoD Component heads, as required, to establish processes and procedures for:

(1) Reporting gaps and issues in DoD IT standards.

(2) Reporting IT standards conformance testing issues.

(3) Proposing to the JESC courses of action to correct reported gaps and issues.

i. Resources DoD IT standards activities to support this issuance and:

(1) Provides the JESC Secretariat to support IT standards governance for DoD and synchronization with the IC.

(2) Provides the hosting IT infrastructure, tools, technical expertise, configuration management, and help desk support.

(3) Implements a process and provides the tools to:

(a) Identify or establish a registry and procedures for tracking DoD Component usage of IT standards, DoD IT standards conformance test results, DoD IT standards compliance waivers, and IT standards gaps and issues.

(b) Provides to the JESC co-chairs 30 days before a JESC Plenary session a report regarding:

1. DoD Component IT conformance test issues.

2. The status of actions to resolve discrepancies and gaps in DoD IT standards or implementation guidance.

3. The status of DoD IT standards compliance waivers.

4. Issues that have arisen since the previous report.

(4) Develops and executes processes and procedures for life-cycle configuration management and periodic review of the DoD IT standards in DISR, IT standards conformance test results, and technical information and guidance. Compiles the DoD Components' reporting

on conformance testing outcomes into a report for JESC co-chairs that reflects DoD IT standards compliance.

(5) Develops, operates, and maintains the online Global Information Grid Technical Guidance – Federation (GTG-F) Suite of Tools.

(6) In coordination with the JESC, identifies the need to adopt or develop new DoD IT standards and recommends retiring obsolete DoD IT standards and standards profiles (StdV-1s).

(7) In coordination with the DoD CIO, the IC Chief Information Officer (CIO), and the JESC co-chairs, establishes and maintains the DoD IT Standards Process Guide. The DoD IT Standards Process Guide will supersede the JESC Standard Operating Procedures and must include procedures for:

(a) JESC operations.

(b) Adoption and distribution of IT standards in the DoD.

(c) Collection and processing of IT standards compliance waivers.

(d) Reporting DoD IT standards conformance test issues.

(e) Identifying, reporting, and resolving gaps and issues in DoD IT standards.

(f) Submitting DoD Architecture Framework (DoDAF)-conformant content for systems.

(g) Providing guidance for conducting IT standards conformance testing.

(h) Out-of-cycle DISR change requests.

(i) Coordinating IT MIL-STDs in accordance with this issuance, DoDI 4120.24 and DoDM 4120.24.

(j) Enforcement and ongoing certification that developed or procured capabilities meet mandated IT standards.

j. Advises DoD Components on selection and application of IT standards that are applicable to their operational needs.

k. Requires that DoDAF-conformant content described in Paragraph 3.7. submitted by a DoD Component for approval is:

(1) Integrated with the functional or system architecture to which it applies.

(2) Employs IT standards that are designated in DISR as “mandated” or “emerging.”

(3) When applicable, includes an approved waiver memorandum in accordance with Paragraph 3.8.

l. Processes all DoD IT standards compliance waivers as described in Paragraph 3.8.

m. Designates a Departmental Standardization Officer and leads efforts to develop IT MIL-STDs that are consistent and aligned across the ASSIST and DISR, in accordance with DoDI 4120.24 and DoDM 4120.24.

(1) In coordination with the DoD Component heads, analyzes all IT MIL-STDs for which a DoD Component will be the preparing activity or lead standardization activity.

(2) Develops procedures for the JESC to engage with the Office of the USD(R&E) Defense Standardization Program Office (DSPO) on development and distribution of IT MIL-STDs.

(3) Provides DSPO an explanation for any IT standards registered in DISR that are not voluntary consensus standards pursuant to the annual reporting requirement of OMB Circular A-119.

(4) Ensures IT MIL-STDs obtain DoD CIO approval and are registered in DISR in accordance with this issuance.

n. Requires that IT standards citations in DISR include references to the repositories that host the associated IT standards' content or artifacts.

o. Coordinates with DSPO to ensure the text of DoD IT MIL-STDs cited in DISR are available in the Office of the USD(R&E)'s ASSIST repository and follow other amplifying policy and procedures outlined in DoDI 4120.24 and DoDM 4120.24.

p. Collaborates with the DoD CIO and DSPO to maintain integrity and accuracy of DoD IT MIL-STD data registered in DISR and the corresponding IT MIL-STD data published in the ASSIST repository.

q. Designates a senior-level Component Standardization Executive to engage with DSPO in coordination with the DoD CIO.

r. Develops technical information and guidance for IT standards in coordination with the DoD Components.

s. Pursuant to DoDD 5101.22E, supports the DoD Executive Agent for the DoD Mission Partner Environment to identify and implement the appropriate IT standards and interoperability testing necessary to integrate information sharing systems and their supporting networks of the United States and mission partners.

t. In coordination with the CJCS and other DoD Component heads, as appropriate, prepares, IT standards agreements needed to ensure system and data interoperability with multinational and interagency capabilities.

2.3. USD(R&E).

In addition to the responsibilities in Paragraph 2.9., the USD(R&E):

a. Manages the Defense Standardization Program to promote standardization of materiel, IT, facilities, and engineering practices in accordance with DoDI 4120.24.

b. Identifies IT standards required to implement the Modular Open System Approach for inclusion in DISR.

c. Collaborates with the DoD CIO and the Director, DISA to maintain integrity and accuracy of DoD IT MIL-STD data published in ASSIST repository and the corresponding IT MIL-STD data registered in DISR.

d. Forms partnerships with appropriate industry associations for use of commercial or non-government standards for replacement of IT MIL-STDs where practicable pursuant to Chapter 223 of Title 10, U.S.C. and DoDD 5137.02.

e. Ensures that advanced technology development activities (i.e., Budget Activity 3) comply and conform with the IT standards in the DISR pursuant to Paragraph 3.7., to ease adoption of new capabilities into the DoD operational environment.

f. Ensures testing, including appropriate IT standards conformance testing, is performed in accordance with DoDI 5000.89 for IT and NSS that are on the OSD Test and Evaluation Oversight List for the USD(R&E). Report a summary of the IT standards conformance testing outcomes pursuant to Paragraph 3.7.

g. Serves as chair for the Modeling and Simulation TWG to champion modeling and simulation IT standards development and adoption in accordance with Section 3 of this issuance.

2.4. USD(A&S).

In addition to the responsibilities in Paragraph 2.9., the USD(A&S):

a. Coordinates with the DoD CIO; USD(R&E); Director, DISA; and the CJCS; and other DoD Component heads, as required, to establish processes and procedures for all acquisition programs regardless of acquisition pathway in order to ensure compliance with this issuance.

b. Where the USD(A&S) is the milestone decision authority (MDA) or decision authority (DA), verifies DoD CAE offices and program managers are accountable for complying and conforming with the IT standards pursuant to Paragraph 3.7.

c. As appropriate, coordinates with the DoD CIO in the DoD IT standards compliance waiver process in Paragraph 3.8.

d. For programs where the USD(A&S) is the MDA or DA, coordinates with the DoD CIO and the CAE on a plan of action and milestones for reaching compliance when an acquisition

program is unable to conform with an applicable IT standard mandated in DISR. The USD(A&S), CAE, and DoD CIO will develop an interim solution that provides a flexible way forward to support the warfighter's immediate needs, ensures interoperability with required capabilities, and achieves full compliance with this issuance by the agreed future milestone.

e. Endorses the DISR baseline memorandum in collaboration with the DoD CIO and CJCS.

2.5. USD(C)/CFO.

In addition to the responsibilities in Paragraph 2.9., the USD(C)/CFO:

a. Requires that budget submissions for IT standards management and compliance costs are included in the DoD Planning, Programming, Budgeting, and Execution process.

b. Requires that all costs needed to support this issuance will be included in appropriate budget exhibit submissions.

2.6. USD(I&S).

In addition to the responsibilities in Paragraph 2.9., the USD(I&S):

a. Coordinates with the IC and interagency security forums on the identification of IT standards to support mission requirements for intelligence, counterintelligence, security associated with the National Intelligence Program, Military Intelligence Program, and other Defense intelligence sources.

b. Directs Defense Intelligence Components and the Defense Security Enterprise to comply and conform with the IT standards in the DISR, pursuant to Paragraph 3.7.

c. Synchronizes and facilitates intelligence information sharing activities across the DoD, the IC, and with mission partners in accordance with DoDD 5143.01.

d. Coordinates with the DoD CIO and the IC CIO on policy and procedures that apply to establishing common IT standards and IT standards unique to their respective DoD and IC authorities.

e. Coordinates with the Interagency Security Committee, the IC, Department of Homeland Security, and other security forums on the identification of IT standards needed to support mission needs for security. Recommends these IT standards be established and registered in the DISR in accordance with this issuance.

2.7. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE.

Under the authority, direction, and control of the USD(I&S); the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor

organization, of the National Security Agency, funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 2.9., the Director, National Security Agency/Chief, Central Security Service, in coordination with the DoD Chief Information Security Officer:

a. Serves as the DoD lead for tactical signals intelligence (SIGINT) standards.

b. Coordinates with the DoD Components to develop tactical SIGINT standards.

c. Ensures that National Security Agency/Central Security Service IT programs comply and conform with IT standards in DISR pursuant to Paragraph 3.7.

d. Coordinates with other appropriate DoD Components, the IC, or other U.S. Government agencies to require that National Security Agency/Central Security Service IT standard profiles for processing foreign intelligence and foreign counterintelligence information will be satisfied by designing and developing interoperable, technical, procedural, operational interfaces pursuant to Paragraph 3.7.

e. Evaluates waiver requests involving information assurance or cybersecurity and SIGINT standards and advises the DoD CIO and DoD Component heads in accordance with Paragraph 3.8.

f. Serves as the U.S. Government's standards focal point for cryptography, telecommunications systems security, and information systems security for NSS.

g. Identifies, develops, and supports, in coordination with the DoD Components through the Information Assurance Cybersecurity TWG, the minimum IT standards, methods, and procedures for protecting cryptographic and other sensitive communications security, information security, and other cybersecurity materials, techniques, and information to be used by all NSS owners. Recommends these IT standards and specifications be established and registered in the DISR in accordance with this issuance.

h. Coordinates with the Director, NIST, to ensure NIST standards are complementary to NSS standards, pursuant to Section 3553 of Title 44, U.S.C.; Executive Order 14028; and NSM-8.

i. Coordinates with the Committee on NSS pursuant to Executive Order 14028 and NSM-8 guidelines to:

(1) Ensure the development of necessary security architectures.

(2) Approve the security standards and doctrine for NSS in accordance with Committee on NSS Directive No. 900.

2.8. DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (DNGA).

Under the authority, direction, and control of the USD(I&S), in accordance with DoDD 5105.60, and in addition to the responsibilities in Paragraph 2.9., the DNGA:

a. Serves as the DoD lead for geospatial intelligence (GEOINT) IT standards.

b. Identifies, develops, and supports, in coordination with the DoD Components through the GEOINT TWG, the standards for GEOINT IT, data, products, and services. These IT standards and specifications are established in accordance with DoDD 5105.60, and are cited in the DISR baseline in accordance with DoDI 5000.56 and this issuance. GEOINT standards are published in the National System for Geospatial-Intelligence Standards Registry.

c. Promotes the adoption of voluntary consensus IT standards from authoritative sources to fulfill requirements for GEOINT standards.

d. Formulates, coordinates, and implements policy for the classification, control, disclosure, and release of GEOINT standards, IT StdV-1, and specifications for the National System for Geospatial Intelligence.

e. Represents the DoD in national and international geospatial information standardization activities.

f. Evaluates waiver requests involving GEOINT standards and advises the DoD CIO and DoD Components in accordance with Paragraph 3.8.

g. Coordinates with the DoD CIO; USD(R&E); USD(A&S); USD(I&S); Director, DISA; and the CJCS; and other DoD Component heads, as required, to establish processes and procedures for enforcing GEOINT standards compliance by designing, developing, or procuring GEOINT capabilities with interoperable technical, procedural, and operational interfaces pursuant to Paragraph 3.7.

2.9. OSD AND DOD COMPONENT HEADS AND THE DIRECTOR, DEFENSE FORENSICS AND BIOMETRICS AGENCY (DFBA).

The OSD and DoD Component heads and the Director, DFBA:

a. Require that IT and NSS in development or procurement:

(1) Use IT standards registered in DISR as mandated or emerging; or

(2) Obtain a DoD IT standards compliance waiver in accordance with Paragraph 3.8.

b. Provide representatives to the JESC in accordance with JESC Charter and Section 3 of this issuance.

c. Provide adequate resources to ensure expert participation in the JESC TWGs and in IT standards activities in Section 3 of this issuance.

d. Ensure that DoD Information Enterprise Architecture's subordinate reference architectures and documents cite only those IT standards registered in DISR in accordance with this issuance.

e. In collaboration with the Software Modernization Senior Steering Group and the JESC, establish processes to identify, develop, and prescribe standards or guidance for applicability for current and emerging commercial software technologies.

f. Identify the need for new or updated IT standards in coordination with the DoD CIO, the USD(R&E), the USD(A&S), and the Director, DISA. Recommend these IT standards be established and registered in the DISR in accordance with Paragraph 3.5.

g. Ensure IT MIL-STDs developed by the Component's preparing activities obtain DoD CIO approval in accordance with this issuance, and are published in ASSIST repository in accordance with DoDM 4120.24.

h. Participate in configuration management of the DISR, including submitting change requests to add and maintain IT standards citations in the DISR via the GTG-F DISR Module as described in Paragraph 3.5.

i. Participate in IT SDOs to influence development of open, consensus-based IT standards that satisfy DoD requirements to enable interoperability, information sharing, reuse, portability, and cybersecurity.

j. Coordinate with the DoD CIO; USD(R&E); USD(A&S); Director, DISA; and, as appropriate, the CJCS; DNGA; Director, National Security Agency/Chief; Central Security Service; and Director, DFBA, to establish processes and procedures for enforcing IT standards compliance.

k. Coordinate with the Director, DISA when developing programmatic and technical guidance to ensure that documents required for IT development and procurement include:

(1) DoDAF-conformant content described in Paragraph 3.7.

(2) IT standards conformance testing.

(3) An IT standard waiver, when required, submitted in accordance with Paragraph 3.8.

l. Require that program managers for DoD IT development or procurement submit standards views and supporting DoDAF-conformant content in accordance with Paragraph 3.7.

m. Where the DoD Component is the MDA or DA, verify CAE offices and program managers are accountable for complying with the IT standards pursuant to Paragraphs 3.7. and 3.8.

n. Coordinate with the DoD CIO and the CAE on a plan of action and milestones for reaching compliance when IT is unable to conform with an IT standard registered in DISR as mandated or emerging. Develop an interim solution that provides a flexible way forward to

support the warfighter's immediate needs, ensures interoperability with required capabilities, and complies with this issuance by the agreed future milestone.

o. Assess compliance with requirements of this issuance in accordance with DoDI 8330.01.

p. Ensure successful DoD IT standards conformance test results, as required to support interoperability, before authorizing connection between the DoD Component's IT systems or networks.

q. Where the DoD Component is the MDA or DA, ensure testing, including appropriate IT standards conformance testing is performed on all developed or procured IT.

r. Advise the DoD CIO, USD(R&E), USD(A&S), Director of Operational Test and Evaluation, CJCS, and Director, DISA, in accordance with reporting procedures in Paragraph 3.7. about:

(1) Successful completion of IT standards conformance test, or instances where significant problems, traceable to IT standards conformance issues, are encountered during developmental or operational interoperability assessments.

(2) Discrepancies or gaps in coverage in DoD IT standards or implementation guidance.

s. Fully support through planning, budgeting, and execution the identification of costs in support of this issuance.

t. Require use of IT standards, including data standards, mandated in DISR to ensure implementation of capabilities for mission partner interoperability and information sharing pursuant to DoDI 8110.01 (e.g., Federated Mission Networking).

u. Ensure implementation of capabilities for mission partner interoperability and information sharing pursuant to DoDI 8110.01.

2.10. SECRETARY OF THE ARMY.

In addition to the responsibilities in Paragraph 2.9., and through the Provost Marshal General and the Director, DFBA, the Secretary of the Army:

a. Serves as the DoD Executive Agent for Forensics in accordance with DoDD 5205.15E and the DoD Executive Agent for Biometrics in accordance with DoDD 8521.01E.

b. Serves as co-chair with Air Force DoD Cyber Crime Center for the DoD Forensic and Biometric TWG to champion forensic and biometric IT standards development within the DoD, U.S. Government, and in international forums.

c. Advocates for DoD interests through active participation in national and international standards bodies and builds consensus on forensics and biometrics IT standards development, evaluation, and implementation.

d. Identifies, develops, and supports, in coordination with the DoD Components through the forensics and biometrics TWG, the applicable standards for IT, data, products, and services. These IT standards and specifications are established in accordance with DoDD 8521.01E and DoDD 5205.15E, and are cited in the DISR baseline, in accordance with DoDI 5000.56 and this issuance.

e. Promotes the adoption of voluntary consensus IT standards from authoritative sources to fulfill requirements for forensic and biometric IT standards.

f. Coordinates with the DoD CIO; USD(R&E); USD(A&S); USD(I&S); Director, DISA; and the CJCS; and other DoD Component heads, as required, to establish processes and procedures to ensure forensics and biometric products, systems, and services adhere to applicable IT standards, protocols, and the DoD forensic and biometric authoritative enterprise reference architecture to support interoperability pursuant to Paragraph 3.7.

g. Evaluates waiver requests involving forensic and biometric IT standards and advises the DoD CIO and the DoD Components in accordance with Paragraph 3.8.

h. Collaborates with the DoD and IC JESC Forensic and Biometric Domain on IT standards recommended for formal adoption in the DISR and, upon adoption, ensures inclusion in the DoD Forensics and Biometrics Reference Architecture StdV-1 and standards forecast (StdV-2).

i. Maintains situational awareness of national and international forensic and biometric IT standards development activities by representing DoD in national and international standards organizations and national organizations (e.g., NIST), and reports on the progress and outcomes of these activities to the DoD community.

2.11. CJCS.

In addition to the responsibilities in Paragraph 2.9. and through the Director, Joint Staff, J6, the CJCS:

a. Coordinates with the DoD CIO, USD(R&E), USD(A&S), and the Director, DISA to require that DoDAF-conformant IT standards viewpoints are included in Joint Capabilities Integration and Development System documentation as described in CJCS Instruction 5123.01 and the Office of the CJCS "Content Guide for the Net-Ready KPP."

b. Provides a sufficiency assessment identifying IT standards, including data standards, and IT StdV-1 required to support joint and combined mission threads.

c. Provides the DoD CIO and the Director, DISA with prioritized military requirements for development and adoption of IT standards to support the DoD.

d. Identifies the need for new IT standards, in coordination with the DoD CIO, USD(R&E), USD(A&S), and the Director, DISA.

e. Coordinates with the DoD CIO; USD(R&E); USD(A&S); and the Director, DISA, and other DoD Component heads, as required, to establish processes and procedures for enforcing IT standards compliance.

f. Coordinates with DoD CIO, as appropriate, in the DoD IT standards compliance waiver process in Paragraph 3.8.

g. Provides representation, in coordination with the other DoD Component heads, to multinational IT standards and data standards organizations and forums for interoperability and information sharing.

h. Supports DoD efforts to mandate and establish IT standards, including data standards, to ensure implementation of capabilities for mission partner interoperability and information sharing pursuant to DoDI 8110.01.

i. Represents the Combatant Commands' concerns in all aspects of DoD IT standards activities.

j. Endorses the DISR baseline memorandum in collaboration with the DoD CIO and USD(A&S).

SECTION 3: PROCEDURES

3.1. DOD IT STANDARDS LIFE-CYCLE.

a. Operational requirements drive the IT standards life-cycle. Accredited, voluntary consensus standards considered for use in the DoD are developed in the public and private sectors with DoD and Federal Government participation. DoD then adopts mission-enabling IT standards for inclusion in the DISR.

b. When requirements cannot be satisfied from existing or emerging IT standards, the DoD initiates action to meet the need through voluntary consensus standards bodies in accordance with Section 272 of Title 15, U.S.C.; OMB Circular A-119; or by developing an IT MIL-STD in accordance with DoDI 4120.24 and DoDM 4120.24.

c. The JESC, the JESC Secretariat, and TWGs ensure IT standards are periodically evaluated for relevance and currency. DISR categorizes an IT standard's status as follows:

(1) Mandated;

(2) Emerging; or

(3) Retired.

d. The "DoD Sunset Date" or "DoD Sunset Event" designation may be assigned to a mandated IT standard as a signal that there is a defined date or event that will lead to the IT standard's retirement. DoD Component developers may use a sunsetted IT standard without submitting a waiver request.

e. DISR also includes information/guidance (I/G) artifacts that are not considered DoD IT standards but are available in DISR as references and are characterized as active or inactive.

3.2. DOD IT STANDARDS GOVERNANCE.

The DoD CIO, in coordination with the IC CIO, established a joint governance structure for IT standards to implement agreements in ODNI/CIO-2009-165. The JESC is the joint governance body that:

a. Oversees the processes for identifying, developing, adopting, establishing, prescribing, and publishing IT standards for use by the DoD and IC.

b. Coordinates with member representatives to develop IT standards and specifications.

c. Advises and supports the DoD CIO and the IC CIO on enterprise IT standards and specifications related to data, services, networks, and security that impact the DoD and IC.

d. Oversees management of the DISR baseline.

e. Recommends IT policies and procedures across the DoD and IC to promote specified enterprise IT standards.

f. Prioritizes IT standards activities in coordination with the Director, Joint Staff, J6. Priorities are based on mission needs and strategic direction consistent with the DoD Digital Modernization Strategy and IC IT Enterprise.

g. Ensures IT standards established in the DISR are periodically evaluated for their currency and relevancy.

h. Promotes application of common enterprise IT standards across the DoD and IC enterprises to enable interoperability of forces.

i. Prescribes the use of mission-enabling IT standards accredited by voluntary consensus standards bodies to enable use of commercial solutions and to reduce resource demands for developing and maintaining IT MIL-STDs.

j. Promotes standardization, interoperability, and scalability of IT among DoD, IC, and other mission partners wherever possible.

3.3. IT SDO PARTICIPATION.

DISA will track and report to the JESC co-chairs about DoD participation in IT SDOs and emerging technologies of interest to the DoD. The annual SDO membership package, approved by the DoD CIO, will be the primary document used. Developed in collaboration with the DoD Components, the SDO membership package will identify DoD representation and resources needed to participate in external Federal, national, and international SDOs.

3.4. DOD IT STANDARDS IDENTIFICATION AND ADOPTION.

a. The order of precedence for identifying, adopting, establishing, and prescribing DoD IT standards, based on OMB A-119 and DoDM 4120.24, is:

(1) IT standards required by Federal law, regulation, policy, or U.S.-ratified international standards agreement.

(2) IT standards developed or adopted by voluntary consensus standards bodies.

(3) Federal IT standards.

(4) IT MIL-STD.

(5) If none of the above sources has an IT standard that meets the need, DISA will initiate action in accordance with Paragraph 3.4.c.

b. The following attributes and characteristics will be considered by the TWGs and JESC when assessing standards for adoption in the DISR:

(1) Utility.

The primary features and functions of this standard meet requirements with minimal to no changes.

(2) Interoperability.

The standard supports 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.

(3) Technical Maturity.

The standard is stable and has well-established marketplace support.

(4) Implementability.

The standard is used in applications within the Federal or private sector.

(5) Security.

The standard, when implemented, would not introduce unacceptable cybersecurity risks to the DoD Information Network.

(6) Applicability.

The standard is relevant and meets the needs of programs. The standard is not expected to cause unacceptable risk with regard to cost, schedule, performance, or security.

(7) Public Availability and Intellectual Property Rights.

The standard is publicly available for unrestricted use and, in accordance with OMB A-119, includes provisions requiring that owners of relevant patented technology incorporated into a standard:

(a) Make that intellectual property available to implementers of the standard on nondiscriminatory and royalty-free or reasonable royalty terms.

(b) Bind subsequent owners of standards-essential patents to the same terms.

c. If no existing IT standard can satisfy the mission need, DISA will:

(1) Confirm the DoD IT standard requirement in coordination with the DoD CIO, USD(R&E), USD(A&S), and the Director, Joint Staff, J6.

(2) Recommend to the JESC a course of action to meet the DoD IT standard requirement such as by initiating action with a voluntary consensus standards body or by initiating an IT MIL-STD development effort in accordance with DoDI 4120.24 and DoDM 4120.24.

(3) Inform the JESC co-chairs on progress and issues.

3.5. ADD OR REVISE A DISR IT STANDARD CITATION.

a. A DoD Component may create a transaction called a "change request" to add or revise a DISR IT standard citation.

b. A DoD Component submits a change request via DISA's GTG-F DISR Module. The GTG-F system controls the process flow of change requests. Each change request first goes through an adjudication process within the DoD Component's organization. The change request is then reviewed by the appropriate TWG. DISA's "Global Information Grid Technical Guidance – Federation DISR Module, Author Users Guide" describes the process of initiating a change request. DISA assesses a user submitted change request to identify, assess, and recommend IT standards to the JESC for inclusion in DISR.

c. DISA will:

(1) Schedule frequent technical exchanges with IT standards developers, users, and DoD Component and IC element representatives to assess change requests and verify that IT standards are current, relevant, and complete.

(2) Coordinate with the DoD and the IC Components to recommend the status categorization of an IT standard as mandated, emerging, or retired.

(3) Coordinate with the DoD and the IC Components to recommend the categorization of an I/G artifact as active or inactive.

(4) Work with DoD Components to identify gaps and issues in DoD IT standards and propose courses of action to the JESC co-chairs.

d. The JESC:

(1) Reviews recommendations of the TWGs in plenary sessions in accordance with the JESC Charter.

(2) Records the votes of all JESC representatives.

(3) Decides whether to change the categorization of a standard (e.g., from emerging to mandated, or from mandated to retired).

(4) Recommends DoD CIO approval of IT standards baselines and updates for incorporation in the DISR.

(5) Ensures gaps and issues in DoD IT standards are identified, tracked, and resolved.

3.6. DOD IT STANDARDS SELECTION BY THE DOD COMPONENTS.

DISA's GTG-F Suite of Tools allows a user to search people, organizations, IT standards, and more. The submitter must use the "Standards-View Wizard" and the "Standards View (STD-V) & GTP Wizard Users Guide" to prepare the StdV-1 and StdV-2.

3.7. DOD IT STANDARDS COMPLIANCE AND CONFORMANCE.

a. Pursuant to Sections 142 and 2223(a)(3) of Title 10, U.S.C., DoD Components developing or procuring DoD IT must use applicable IT standards, including data standards, that are prescribed by the DoD CIO in the DISR as mandated or emerging. Use of applicable DoD CIO-mandated or emerging IT standards enables interoperability, information sharing, reuse, portability, cybersecurity, and innovation.

b. Use of an IT standard that is not registered in DISR as mandated or emerging requires a DoD IT standards compliance waiver approved in accordance with Paragraph 3.8.

c. In addition to a DoD Component's internal review of IT standards compliance, IT standards compliance is also reviewed during:

(1) The DoD capabilities process in accordance with CJCS Instruction 5123.01.

(2) The acquisition process in accordance with DoDD 5000.01.

(3) The interoperability certification process in accordance with this issuance and DoDI 8330.01.

d. To support the review of DoD IT standards conformance, DoD Components use the GTG-F Suite of Tools to submit the following DoDAF-conformant content described in the DoD CIO-approved DoDAF Architecture Framework:

(1) StdV-1 and StdV-2 developed using the GTG-F Standards-View Wizard and the DoDAF-conformant content (e.g., SV-6 or SvcV-6) to which each IT standard applies.

(2) Operational Resource Flow Matrix (i.e., OV-3).

(3) Systems Resource Flow Matrix (i.e., SV-6) or Services Resource Flow Matrix (i.e., SvcV-6) that cite applicable IT standards for each system resource flow exchanged between systems or services.

e. Coordinate with Joint Interoperability Test Command to determine if other architecture viewpoints (e.g., Data and Information Viewpoint-1, 2, or 3) may be needed to ensure requirements are sufficiently complete, detailed, measurable, and testable.

f. Acquisition, system engineering, and test planning documentation must address conformance with applicable IT standards.

g. IT standards conformance is confirmed through testing to evaluate whether DoD IT fulfills the requirements of the applicable IT standards mandated in the DISR.

(1) The DoD Components must conduct IT standards conformance testing during development and integration processes.

(2) The DoD Components will advise DISA in accordance with Paragraph 3.9. about interoperability discrepancies that are traceable to an issue with the IT standard citation or specification.

(3) DISA will compile the DoD Component inputs into a report for the DoD CIO that reflects IT standards conformance for the DoD.

(4) DISA will track DoD IT standards conformance test outcomes and report standards conformance test issues to the JESC co-chairs.

(5) When a DoD Component discovers an issue or problem with an IT standard during conformance testing, the DoD Component will notify the JESC Secretariat so the issue can be fixed.

(6) The JESC co-chairs and JESC Secretariat will develop and execute a course of action to resolve gaps and issues in DoD IT standards and track them to resolution.

h. The interoperability certification authority, as established by DoDI 8330.01, assesses conformance with IT standards as part of the interoperability certification process.

3.8. DOD IT STANDARDS COMPLIANCE WAIVERS.

a. Pursuant to Section 142 of Title 10, U.S.C., DoD Components may not develop or procure IT that does not fully comply with such standards as the DoD CIO may establish.

b. A DoD Component developing or procuring DoD IT must obtain the DoD CIO approval or an authorized DoD Component MDA's approval before using a DoD IT standard that is not registered in DISR as mandated or emerging. The DoD Component prepares a DoD IT standards compliance waiver request in accordance with the "DoD IT Standards Compliance Waiver Request Instructions" accessible on the GTG-F website. The waiver request provides visibility of potential gaps and functional discrepancies in DoD IT standards that need to be resolved and includes:

(1) A justification for using an IT standard that is not registered in DISR as mandated or emerging.

(2) The risks of using the non-compliant standard.

(3) How the risks of using the non-compliant standard will be mitigated.

(4) A plan of action and milestones for bringing the DoD IT into compliance by using an applicable mandated or emerging standard.

c. The requesting DoD Component then submits the waiver request to the DoD CIO or an authorized DoD Component MDA for review and approval. The DoD CIO or an authorized DoD Component MDA may approve the use of an IT standard registered in DISR as retired. Due to increased risk, only the DoD CIO can approve a waiver to use an IT standard that is not registered in DISR.

d. To obtain DoD CIO approval to use an IT standard that is not registered in DISR as mandated or emerging, the requesting DoD Component:

(1) Submits the DoD IT standards compliance waiver request to the JESC Secretariat. If the waiver request or any supporting information is classified, the requesting DoD Component must coordinate with the JESC Secretariat for submission procedures.

(2) Upon receipt, the JESC Secretariat will forward the waiver request to the JESC stakeholders for the IT standard (e.g., National Geospatial-Intelligence Agency, National Security Agency/Central Security Service, DFBA, or the appropriate JESC TWG) for review.

(3) The JESC stakeholders for the IT standard will forward a technical analysis and recommendation to the JESC Secretariat.

(4) The JESC Secretariat will make a final recommendation within 25 working days to:

(a) The DoD CIO for a DoD Component IT standards waiver request;

(b) The IC CIO for IC IT standards waiver requests; or

(c) Both the DoD CIO and IC CIO where the standard or policy being waived involves both DoD and IC equities.

(5) A waiver request may be approved or rejected. The decision may include a rationale for a rejected waiver request or any conditions associated with an approved waiver request. The JESC Secretariat will provide the decision to the requesting DoD Component.

(6) JESC Secretariat will track to resolution any gaps or issues in DoD IT standards or implementation guidance identified in a DoD Component's waiver requests.

(7) The requesting DoD Component, in coordination with the JESC Secretariat, will ensure the system's StdV-1, all DoD CIO or MDA approved IT standards compliance waivers, and supporting DoDAF-conformant content specified in Paragraph 3.7. are accessible on the GTG-F website.

e. To obtain an authorized DoD Component MDA's approval to use a standard registered in DISR as retired, the requesting DoD Component:

(1) Prepares a DoD IT standards compliance waiver request and submits it to the authorized DoD Component MDA.

(2) If the waiver request is approved by the authorized DoD Component MDA, the requesting DoD Component must submit the MDA-approved waiver to the JESC Secretariat within 30 days of approval.

(3) The requesting DoD Component, in coordination with the JESC Secretariat, will ensure the system's StdV-1, StdV-2, all DoD CIO or MDA-approved IT standards compliance waivers, and supporting DoDAF-conformant content specified in Paragraph 3.7. are accessible on the GTG-F website. If the MDA-approved waiver request or any supporting information is classified, the requesting DoD Component must coordinate with the JESC Secretariat for submission procedures.

3.9. IDENTIFYING GAPS AND ISSUES INVOLVING DOD IT STANDARDS.

A DoD Component that identifies a gap or issue involving DoD IT standards will work with the DoD Component JESC representative or the JESC Secretariat to determine the best approach for addressing the gap or issue. The list of DoD Component JESC representatives is accessible on the GTG-F Suite of Tools Website. Resolution of the gap or issue may require the DoD Component to submit a change request as described in Paragraph 3.5. to resolve the gap or issue.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CAE	Component Acquisition Executive
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
DA	decision authority
DBS	defense business systems
DFBA	Defense Forensics and Biometrics Agency
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry
DNGA	Director, National Geospatial-Intelligence Agency
DoD CIO	DoD Chief Information Officer
DoDAF	DoD Architecture Framework
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DSPO	Defense Standardization Program Office
GEOINT	geospatial intelligence
GTG-F	Global Information Grid Technical Guidance – Federation
IC	intelligence community
I/G	information/guidance
IT	information technology
JESC	Joint Enterprise Standards Committee
MDA	milestone decision authority
MIL-STD	military standard
NIST	National Institute of Standards and Technology
NSM	National Security Memorandum
NSS	national security systems
ODNI/CIO	Office of the Director of National Intelligence Chief Information Officer
OMB	Office of Management and Budget
SDO	standards development organization
SIGINT	signals intelligence
StdV-1	standards profile

ACRONYM	MEANING
StdV-2	standards forecast
TWG	technical working group
U.S.C.	United States Code
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

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

TERM	DEFINITION
accredited standard	A published standard from a recognized SDO that has an established position within the relevant technical, professional, and marketplace communities as an objective authority in its sphere of activity (e.g., the International Organization for Standardization, the American National Standards Institute, the International Telecommunication Union).
advanced technology development	Defined in Volume 2B of DoD 7000.14-R.
ASSIST	Defined in DoDM 4120.24.
Business Mission Area	Defined in DoDI 8115.02.
cybersecurity	Defined in DoDI 8510.01.
DBS	Defined in Section 2222 of Title 10, U.S.C.
Defense Security Enterprise	Defined in DoDD 5200.43.
Defense Standardization Program	Defined in DoDI 4120.24.
Digital Modernization Infrastructure Executive Committee	Defined in the DoD CIO's "Charter for the Digital Modernization Infrastructure Executive Committee."

TERM	DEFINITION
DISR	The authoritative registry that identifies DoD IT and NSS standards prescribed for use across the DoD pursuant to Sections 142 and 2223(a)(3) of Title 10, U.S.C. The DISR is accessed through the GTG-F Suite of Tools.
DoDAF-conformant content	Defined in the DoD CIO's DoDAF Architecture Framework.
DoD Information Enterprise	Defined in DoDD 8000.01.
DoD Information Enterprise Architecture	The architecture, standards, and organizing framework for describing the DoD desired Information Enterprise and for guiding the development of the DoD IT capabilities.
DoD IT standards	Common and repeated use of rules, conditions, guidelines or characteristics for: processes; procedures; practices; operations; services; interfaces; connectivity; interoperability; and data or information formats for information interchange, transmission, or transfer.
DoD IT standards compliance waiver	An approval to implement an IT standard that does not fully comply with provisions of this issuance. Waivers may provide indicators of potential interoperability problems and visibility of potential gaps or functional discrepancies in DoD IT standards that need to be resolved.
emerging IT standard	An IT standard that is established and approved by the DoD CIO for use across the DoD for the development or procurement of a DoD IT capability to which it applies. An emerging IT standard is in its final stages of development and is under consideration as a mandated DoD IT standard. It does not require an IT standards compliance waiver.
enterprise architecture	Defined in OMB Circular A-130.
GEOINT	Defined in DoDD 5105.60.
GTG-F Suite of Tools	The online guidance and associated processes and documentation that support the preparation,

TERM	DEFINITION
	submission, verification, assessment, review, approval, and selection of IT standards.
I/G	An artifact registered in DISR that provides additional information or guidance not covered in the IT standards citation or specification for implementing an IT standard. An I/G is not a DoD IT standard. Examples are: IT policy memos, IT procedures, IT best common practices, and IT manuals. I/G entries in DISR are categorized as active or inactive.
information system	Defined in Section 3502 of Title 44 U.S.C.
interoperability	Defined in DoDI 8330.01.
IT	Defined in the Committee on NSS Instruction No. 4009.
IT MIL-STD	A DoD-unique IT standard developed after first assessing existing commercial open-industry IT Standards and voluntary consensus standards and finding no solution. DoD-unique IT standards are developed by a DoD preparing activity to support the DoD mission requirement. Development of an IT MIL STD is done in accordance with Section 272 of Title 15, U.S.C., OMB Circular A-119, DoDI 4120.24, and DoDM 4120.24. An IT MIL-STD citation is registered in DISR as mandated, emerging, or retired in accordance with this issuance. The text of an IT MIL-STD is published in the ASSIST repository in accordance with DoDM 4120.24.
IT services	Defined in DoDI 8320.07.
IT standard	Common and repeated use of rules, conditions, guidelines or characteristics for IT: processes; procedures; practices; operations; services; interfaces; connectivity; interoperability; and data or information formats for information interchange, transmission, or transfer.

TERM	DEFINITION
IT standard categories	An indication in the DISR of the technical maturity of a standard, or version of a standard, and its utility in the current technology environment. DISR standard categories are: mandated, emerging, or retired.
IT standards conformance test	A program or procedure designed to obtain, verify, or provide data for the evaluation of whether IT conforms with a standard cited in the DISR.
JESC	The DoD IT standards governance structure that is established in the JESC Charter.
JESC Secretariat	Members of the JESC who provide administrative support for the day-to-day operations, coordination, and execution of JESC governance activities on behalf of the DoD CIO and IC CIO. The JESC Secretariat comprises DoD and IC personnel dedicated to providing the necessary support.
Joint Capabilities Integration and Development System	Defined in CJCS Instruction 5123.01.
lead standardization activity	Defined in DoDM 4120.24.
mandated IT standard	An IT standard that is established and required by the DoD CIO for use across the DoD for the development or procurement of a DoD IT capability to which it applies.
MDA	Defined in DoDD 5135.02.
mission partner	Defined in DoDD 5101.22E.
mission partner environment	Defined in DoDD 5101.22E.
Modular Open System Approach	Defined in Section 4401(b)(1) of Title 10, U.S.C.
NSS	Defined in Executive Order 14028.
preparing activity	Defined in DoDM 4120.24.

TERM	DEFINITION
retired IT standard	An IT standard that is no longer approved by DoD CIO for developing or procuring DoD IT. Use of a retired IT standard when developing or procuring DoD IT requires a waiver in accordance with Paragraph 3.8. Retired IT standard citations remain in the DISR for reference.
SDO	A domestic or international organization that plans, develops, establishes, or coordinates voluntary consensus standards using procedures that incorporate the attributes of openness, balance of interests, due process, an appeals process, and consensus in a manner consistent with OMB Circular A-119.
security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems.
specification	An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional requirements, and architectural designs) associated with an information system.
standard citation	The metadata regarding each IT standard cited in the DISR. This metadata includes information on the purpose and use of the standard and information on where the full standard is recorded.
standards conformance	Confirmation by testing that IT fulfills the requirements of applicable IT standards cited in the DISR.
standards compliance	The verification and validation that documentation for a system, product, IT services, or interface complies with the policy in this issuance.
standards conformance	Confirmation by testing that IT fulfills the requirements of applicable IT standards cited in the DISR.

TERM	DEFINITION
StdV-1	The listing of standards that apply to solution elements. The DoDAF StdV-1 defines the technical, operational, and business standards, guidance, and policy applicable to the architecture being described, as well as identifying applicable technical standards. The DoDAF StdV-1 also documents the policies and standards that apply to the operational or business context.
StdV-2	The description of emerging standards and potential impact on current solution elements within a set of time frames. The StdV-2 contains expected changes in technology-related standards, operational standards, or business standards and conventions, which are documented in the StdV-1 model.
technical standard	A common and repeated use of rules, conditions, guidelines or characteristics for products or related processes and production methods, and related management systems practices.
TWG	A team composed of DoD and IC technical and functional subject matter experts established by the JESC that is primarily responsible for analysis, evaluation, and resolution of technical issues, and providing recommendations about IT standards citations for JESC consideration. The current JESC TWGs are listed at: https://gtg.csd.disa.mil/disr/admin/twg/search.html.
voluntary consensus standard	A standard that is prepared by an authoritative voluntary consensus standards body and is publicly available. Patents, copyrights, intellectual property right constraints, and royalty provisions and intellectual property contained in voluntary consensus standards are made available on a non-discriminatory, royalty-free, or reasonable royalty basis to all interested parties.
voluntary consensus standards bodies	A type of association, organization, or technical society that plans, develops, establishes, or coordinates voluntary consensus standards using a voluntary consensus standards development process that includes the following attributes or elements:

TERM	DEFINITION
	openness, balance, due process, appeals process, consensus. Examples include: American National Standards Institute, International Organization for Standardization, and the Internet Engineering Task Force.
waiver	An approved exclusion or deviation from a requirement as specified in this issuance.

REFERENCES

American National Standards Institute, "U.S. Standards Strategy," 2020 edition[1]

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

Committee on NSS Directive No. 900, "Governing and Operating Procedures," May 9, 2013

Committee on NSS Instruction No. 4009, "Glossary," March 2, 2022

Defense Information Systems Agency, "DoD IT Standards Compliance Waiver Request Instructions," current version[2]

Defense Information Systems Agency, "Global Information Grid Technical Guidance – Federation DISR Module," current edition[3]

Defense Information Systems Agency, "Global Information Grid Technical Guidance – Federation DISR Module, Author Users Guide," current edition[4]

Defense Information Systems Agency, "Global Information Grid Technical Guidance – Federation Suite of Tools," current edition[5]

Defense Information Systems Agency, "Standards View (STD-V) & GTP Wizard Users Guide," current version[6]

Defense Information Systems Agency, Standards-View Wizard online[7]

DoD 7000.14-R, Volume 2B, "DoD Financial Management Regulation: Budget Formulation and Presentation," June 2004, as amended[8]

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

DoD Directive 5101.22E, "DoD Executive Agent (DoD EA) for DoD Mission Partner Environment (MPE)," August 5, 2020

DoD Directive 5105.60, "National Geospatial-Intelligence Agency (NGA)," July 29, 2009

DoD Directive 5135.02, "Under Secretary of Defense for Acquisition and Sustainment USD(A&S))," July 15, 2020

DoD Directive 5137.02, "Under Secretary of Defense for Research and Engineering (USD(R&E))," July 15, 2020

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

---

[1] https://www.ansi.org/resource-center/publications-subscriptions/usss
[2] https://gtg.csd.disa.mil/uam/support/userDocument/list (Scroll down to find the "Waiver Request Instructions")
[3] https://gtg.csd.disa.mil/disr/dashboard.html
[4] https://gtg.csd.disa.mil/uam/support/userDocument/list (Scroll down to find the "DISR Users Guide – Author")
[5] https://gtg.csd.disa.mil
[6] https://gtg.csd.disa.mil/uam/support/userDocument/list (Scroll down to find the "Standards View (STD-V) & GTP Wizard Users Guide")
[7] https://gtg.csd.disa.mil/uam/homepage (Select "Access STD-V Wizard")
[8] https://comptroller.defense.gov/Portals/45/documents/fmr/archive/02barch/02b_05old.pdf

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

DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1, 2012, as amended

DoD Directive 5205.15E, "DoD Forensic Enterprise (DFE)," April 26, 2011, as amended

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

DoD Directive 8521.01E, "DoD Biometrics," January 13, 2016, as amended

DoD Instruction 4000.19, "Support Agreements," December 16, 2020

DoD Instruction 4120.24, "Defense Standardization Program," March 31, 2022

DoD Instruction 5000.56, "Programming Geospatial-Intelligence (GEOINT), Geospatial Information and Services (GI&S), and Geodesy Requirements for Developing Systems," July 9, 2010, as amended

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

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

DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended

DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011, as amended

DoD Instruction 8110.01, "Mission Partner Environment Information Sharing Capability Implementation for the DoD," June 30, 2021

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

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

DoD Instruction 8330.01, "Interoperability of Information Technology, Including National Security Systems," September 27, 2022

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

DoD Manual 4120.24, "Defense Standardization Program (DSP) Procedures," September 24, 2014, as amended

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

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

Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011

Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021

Headquarters Department of the Army General Orders No. 2016-08, "Redesignation and Transfer of the Biometric Identity Management Agency as the Defense Forensics and Biometrics Agency," 28 April 2016[9]

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

National Geospatial-Intelligence Agency, "National System for Geospatial-Intelligence Standards Registry"[10]

National Security Memorandum 8, "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," January 19, 2022[11]

North Atlantic Treaty Organization, Federated Mission Networking online guidance[12]

Office of the DoD Chief Information Officer, "Charter for the Digital Modernization Infrastructure Executive Committee," 13 July 2020

Office of the Chairman of the Joint Chiefs of Staff, "Content Guide for the Net-Ready KPP," current edition[13]

Office of the Director of National Intelligence Chief Information Officer ODNI/CIO-2009-165, "Memorandum of Agreement (MOA) for Coordinated Enterprise Standards Governance," June 9, 2009

Office of the DoD Chief Information Officer, "DoD Architecture Framework," current version[14]

Office of the DoD Chief Information Officer and Office of the Intelligence Community Chief Information Officer, "Joint Enterprise Standards Committee Charter," January 23, 2023[15]

Office of Management and Budget Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities," January 22, 2016, as revised[16]

Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource," July 28, 2016[17]

Office of Management and Budget, United States Trade Representative, and Office of Science and Technology Policy Joint Memorandum M-12-08, "Principles for Federal Engagement in Standards Activities to Address National Priorities," January 17, 2012

Office of the Under Secretary of Defense for Research and Engineering, "ASSIST" online repository[18]

---

[9] https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN7191_go1608_Final.pdf
[10] https://nsgreg.nga.mil
[11] https://www.govinfo.gov/content/pkg/DCPD-202200025/pdf/DCPD-202200025.pdf
[12] https://dnbl.ncia.nato.int/FMNPublic
[13] https://intellipedia.intelink.gov/wiki/Content_Guide_for_the_Net-Ready_KPP
[14] https://dodcio.defense.gov/Library/DoD-Architecture-Framework/
[15] https://gtg.csd.disa.mil/uam/support/policyGuidance/view?id=19
[16] https://www.whitehouse.gov/wp-content/uploads/2020/07/revised_circular_a-119_as_of_1_22.pdf
[17] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[18] https://assist.dla.mil/online/start/

Public Law 108-237, "Standards Development Organization Advancement Act of 2004," June 22, 2004

United States Code, Title 10

United States Code, Title 15, Section 272

United States Code, Title 44