Department of Defense
INSTRUCTION

NUMBER 8310.aa

DoD CIO

SUBJECT: Information Technology Standards in the DoD

References: See Enclosure 1

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

a. Establishes policy, assigns responsibilities, and provides direction for identifying, developing, and prescribing DoD standards for information technology (IT), to include national security systems (NSS) and defense business systems (DBS), pursuant to section 2223 of Title 10, United States Code (U.S.C.) (Reference (c)).

b. Delineates the responsibilities of the Director, Defense Information Systems Agency (DISA) as DoD Executive Agent (EA) for IT Standards, in accordance with DoDD 5105.19 (Reference (d)).

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) All IT, to include NSS and DBS (referred to in this instruction as "IT") systems or services, as defined in DoD Instruction (DoDI) 8320.02 (Reference (e)), that any DoD Component plans, designs, develops, acquires, sponsors, or uses, including:

(a) IT that shares, exchanges, and uses information to enable units or forces to operate in joint, multinational, or interagency operations.

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

DRAFT

(c) IT that supports DoD mobility initiatives to include infrastructure, applications, services, and management.

(3) External organizational entities, by mutual agreements, conducting activities with the DoD, including:

(a) Non-government organizations, both commercial and nonprofit.

(b) Federal agencies of the U.S. government and State, local, and tribal government entities other than the DoD.

(c) Foreign national governments.

(d) International government organizations.

b. Nothing contained in this instruction is construed to limit the authority of a Milestone Decision Authority (MDA) to issue an Acquisition Decision Memorandum that may, where authorized and appropriate, include waivers of requirements, standards, or policy, as deemed appropriate by the MDA. The MDA provides for the acquisition of joint urgent operational needs and other urgent operational needs, and for exploratory development activities not withstanding other provisions of this policy.

c. This instruction does not alter or supersede existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information and Special Access Programs for intelligence pursuant to Executive Order 12333 (Reference (f)), national security information systems pursuant to Executive Order 13231 (Reference (g)), and other laws and regulations.

d. This instruction does not apply to cleared contractors' information systems processing classified information under the National Industrial Security Program, which are subject to certification and accreditation by the Defense Security Service in its role as the Designated Approving Authority in accordance with DoDI 5220.22 (Reference (h)).

3. POLICY. It is DoD policy that:

a. IT standards and standards profiles will be identified, developed, and prescribed for use throughout the DoD to promote interoperability, information sharing, reuse, portability, and cybersecurity within the DoD, as well as with federal agencies and multinational partners.

b. DoD-approved and adopted standards will be listed in the DoD IT Standards Registry (DISR) to be selected by programs as part of their acquisition milestone preparation process or when upgrading fielded systems. Those programs with approved standards baselines will be encouraged, but are not required, to use the latest approved version of an IT standard.

c. IT standards will be governed in accordance with section 3 of Enclosure 3 of this instruction to identify, develop, and prescribe IT standards to promote interoperability,

information sharing, reuse, portability, and cybersecurity across the DoD in accordance with the Joint Enterprise Standards Committee (JESC) Charter (Reference (i)).

d. IT standards not mandated in law or federal regulation will be considered from development sources in the Table in Enclosure 3 of this instruction.

e. Intra-agency and interagency support agreements in accordance with DoDI 4000.19 (Reference (j)) and other necessary arrangements, as required, may be used to fulfill assigned responsibilities, roles, and authorities delineated in this instruction.

f. IT standards support the development and operation of the Joint Information Environment (JIE).

g. IT standards will support and follow information and physical security policy guidance.

h. IT standards will support federal interoperability for physical access control in accordance with Office of Management and Budget (OMB) Memorandum M-11-11 (Reference (k)).

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.

7. EFFECTIVE DATE. This instruction:

a. Is effective [Directives Division will insert date upon publishing to the website].

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

c. Will expire effective [10 YEARS FROM PUBLICATION DATE - Directives Division will insert date upon publishing to the website] and be removed from the DoD Issuances Website if it hasn't been reissued or cancelled in accordance with Reference (l).

Terry A. Halvorsen
Acting Department of Defense
Chief Information Officer

DRAFT

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

DRAFT

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES 6

ENCLOSURE 2: RESPONSIBILITIES 8

DoD CHIEF INFORMATION OFFICER (DoD CIO) 8
DIRECTOR, DISA 9
USD(AT&L) 12
UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO) 13
USD(I) 13
DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS) 13
DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA) 14
OSD AND DoD COMPONENT HEADS 15
CJCS 16

ENCLOSURE 3: PROCEDURES 18

PURPOSE 18
IT STANDARDS LIFE-CYCLE 18
DoD IT STANDARDS GOVERNANCE 18
IT SDO MANAGEMENT 19
IT STANDARDS ADOPTION AND DEVELOPMENT 20
Adoption of IT Standards 20
New Standards Development 21
IT STANDARDS MANAGEMENT 21
IT STANDARDS COMPLIANCE AND CONFORMANCE 22
Use of Mandated Standards 22
Use of Mandated Standards Profiles 22
IT Standards Compliance 22
IT Standards Conformance 23
WAIVERS TO DoD IT STANDARDS POLICY 23

GLOSSARY 25

PART I: ABBREVIATIONS AND ACRONYMS 25
PART II: DEFINITIONS 26

TABLE

DoD Standards Consideration 20

DRAFT

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," April 22, 2013
(b) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
(c) Title 10, United States Code
(d) DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," July 25, 2006
(e) DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
(f) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(g) Executive Order 13231, "Critical Infrastructure Protection in the Information Age," October 16, 2001, as amended
(h) DoDI 5220.22, "National Industrial Security Program (NISP)," March 18, 2011
(i) Joint Enterprise Standards Committee Charter, March 28, 2013[1]
(j) DoD Instruction 4000.19, "Support Agreements," April 25, 2013
(k) OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors," February 3, 2011
(l) DoD Instruction 5025.01, "DoD Issuances Program," June 6, 2014, as amended
(m) Public Law 108-237, "Standards Development Organization Advancement Act of 2004," June 22, 2004
(n) Public Law 104-113, "National Technology Transfer and Advancement Act of 1995," March 7, 1996
(o) Office of Management and Budget Circular A-119 Revised, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities," February 10, 1998
(p) 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
(q) Office of Management and Budget Circular A-130, "Management of Federal Information Resources," February 8, 1996, as amended
(r) DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006
(s) DoD Instruction 4120.24, "Defense Standardization Program (DSP)," July 13, 2011
(t) DoD 4120.24-M, "Defense Standardization Program (DSP) Policies and Procedures," September 24, 2014
(u) Interim DoD Instruction 5000.02, "Operation of the Defense Acquisition System," November 25, 2013
(v) DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010
(w) Title 44, United States Code

[1] Available at http://www.gwg.nga.mil/documents/JESC Charter Signed 2013 03 28.pdf

DRAFT

(x) Committee on National Security Systems (CNSS) Directive No. 900, “Governing and Operating Procedures,” May 9, 2013[2]
(y) DoD Directive 5105.60, “National Geospatial-Intelligence Agency (NGA),” July 29, 2009
(z) DoD Architecture Framework, Version 2.02, August 2010[3]
(aa) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)", May 21, 2014
(ab) Defense Acquisition Guidebook, current version[4]
(ac) Chairman of the Joint Chiefs of Staff Instruction 3170.01H, “Joint Capabilities Integration and Development System,” January 10, 2012
(ad) DoD Directive 5000.01, “The Defense Acquisition System,” May 12, 2003, as amended
(ae) Title 40, United States Code

DRAFT

[2] Available at https://www.cnss.gov/CNSS/openDoc.cfm?I7Dce7ZUWi2ZpUfc/ILdAg==
[3] Available at http://dodcio.defense.gov/dodaf20.aspx
[4] Available at https://dag.dau.mil/Pages/Default.aspx

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CHIEF INFORMATION OFFICER (DoD CIO). In addition to the responsibilities in section 8 of this enclosure, the DoD CIO:

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

b. Establishes and maintains, in coordination with the DoD Components, policy and processes for identifying, developing, and prescribing IT standards that apply throughout the DoD, in accordance with:

(1) Reference (j).

(2) Section 2223 of Reference (c).

(3) Public Law 108-237 (Reference (m)).

(4) Public Law 104-113 (Reference (n)).

(5) OMB Circular A-119 (Reference (o)).

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

(7) OMB Circular A-130 (Reference (q)).

c. Uses the DoD CIO Executive Board (EB) governance structure to provide direction, oversight, and priorities for prescribing IT standards across the DoD.

d. Coordinates with the Intelligence Community (IC) CIO and the Under Secretary of Defense for Intelligence (USD(I)) to develop policy and procedures that apply to the prescription of IT standards for DoD and the IC.

e. Provides oversight, with the DoD Components and the IC, for the development and maintenance of the DISR.

f. Approves waivers to use other than mandated or emerging standards in accordance with section 8 of Enclosure 3.

g. Oversees, through the JESC, use of IT standards in DoD that are not developed or adopted by a voluntary consensus standards body.

DRAFT

h. Coordinates with the IC CIO and the USD(I) to establish a community-based forum and IT standards governance structure to collaborate on common standards, DoD and IC-unique standards, profiles, and other specifications for the respective information environments.

i. Appoints the DoD co-chair for the JESC.

j. Coordinates with mission area leads, in accordance with DoDI 8115.02 (Reference (r)), to participate in the IT Standards Program (ITSP).

k. Provides, in coordination with the DoD Components, annual direction and guidance to the DoD EA for IT Standards on ITSP objectives, priorities, and outcomes.

l. Coordinates DoD IT standards activities at the federal executive level.

m. Provides oversight to synchronize DoD IT standards management with the development and operation of the JIE.

n. Establishes processes and procedures for oversight of IT standards compliance in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the USD(I), the DoD EA for IT Standards, and the CJCS and other DoD Component heads, as required.

o. Approves the annual standards development organization (SDO) membership package submitted by the DoD EA for IT Standards.

p. Confirms DoD need for new IT standards in coordination with the DoD EA for IT standards, the USD(AT&L), and the CJCS.

q. Requires that funds and costs needed to support the DoD ITSP be identified and recommends that they be included in the IT budget.

r. Oversees Business Enterprise Architecture compliance with DoD IT standards in the DISR for DBS.

s. Develops and maintains, as appropriate, a set of Business Mission Area IT standards and specifications for data and services supporting financial, human resources, acquisition, logistics, installations, and defense security business processes.

t. Submits all Business Mission Area IT standards and specifications to the DISR.

2. DIRECTOR, DISA. Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in section 8 of this enclosure, the Director, DISA:

DRAFT

a. Serves as the DoD EA for IT Standards, in accordance with Reference (d), and is responsible for coordinating with the DoD Component heads, as appropriate, to identify and propose IT standards that apply throughout the DoD.

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

c. Develops, maintains, and executes the DoD ITSP, in coordination with the DoD Components and the IC.

d. Prepares and maintains, in coordination with the DoD Component heads, as appropriate, and with DoD CIO approval, an annual SDO membership package. This package will identify which SDOs the DoD will acquire memberships from and designate representatives to attend and take part in these SDOs to represent the DoD's interests.

e. Provides the infrastructure, resources, and tools required to support the ITSP execution, to include configuration management, compliance costs, hosting environments, and help desk support.

(1) Maintains the DISR that enables process and procedures for life-cycle configuration management (periodic review and affirmation) of mandated, emerging, and retired IT standards, technical guidance resources, and standards profiles to support the development and fielding of IT. Periodically reviews the registry to verify that each standard is current. Publishes the DISR standard operating procedure (SOP) to detail adoption and distribution of standards in the DoD.

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

f. Identifies, with the DoD Components, open (voluntary consensus) IT standards from authoritative sources, including military standards (MIL-STDs), if required, for inclusion in the DISR.

g. Leads, with the DoD Components and the Defense Standardization Program (DSP) Office, efforts to develop DoD-unique IT MIL-STDs.

(1) Develops, with the DoD Components, IT MIL-STDs only when public and private sector open (voluntary consensus) IT standards do not meet DoD needs in accordance with References (n) and (o).

(2) Conducts, with the DoD Components, analysis on all standards for which a DoD Component will be the preparing activity (PA) or lead standardization activity (LSA), in accordance with DoDI 4120.24 and DoD 4120.24-M (References (s) and (t)).

h. Appoints the DoD representatives to take part in external public and private sector technical standards forums, and oversees DoD representation at multinational IT standards organizations.

DRAFT

(1) Maintains membership in, and provides DoD standards needs to, public and private IT sector standards development and setting activities.

(2) Establishes DoD positions on IT standards issues in external forums.

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

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

(5) Supports the DoD CIO in execution of IT standards, guidance, direction, and oversight of the ITSP at the federal executive level.

i. Influences the development of commercial off-the-shelf products that satisfy DoD IT standards requirements in accordance with federal policy and U.S. National Standards Strategy.

j. Prepares, in coordination with the DoD Component heads, as appropriate, IT standards agreements for multinational and interagency interoperability.

k. Provides administrative support for JESC secretariat activities and operation of the DISR.

l. Helps the DoD Components identify and use prescribed IT standards and mandated IT standards profiles.

m. Coordinates with the DoD CIO, the USD(AT&L), and the CJCS and other DoD Component heads to establish processes and procedures for IT standards compliance.

n. Confirms that test documentation, information system security plans, and information support plans (ISPs) identify mandated standards profiles needed for IT standards compliance.

o. Conducts associated standards profile reviews and provides recommendations to the USD(AT&L); the DoD CIO; the Director, Operational Test and Evaluation; and the CJCS.

p. Requires that DoD IT MIL-STDs and military specifications cited in the DISR are in the DSP Acquisition Streamlining and Standardization Information System (ASSIST) database at https://assist.dla.mil/online/start/ and follow other amplifying policy and procedures outlined in References (s) and (t).

q. Requires that DISR citations for other DoD and federally developed standards include the associated registries for the standard content or artifact (e.g., National Information Exchange Model and the Data Services Environment registries).

r. Provides technical support to the JESC, the DoD CIO, the USD(AT&L), and the CJCS in the development of new DoD IT standards.

DRAFT

s. Collaborates with military and external federal, national, and international standards bodies to identify emerging standards.

t. Develops technical guidance, including IT standards profiles, in coordination with the DoD Components.

u. Supports development, in coordination with the DoD CIO and the IC CIO, of the JESC SOP for approval by the JESC.

v. Processes all waivers to this instruction requiring DoD CIO approval in accordance with section 8 of Enclosure 3.

w. Helps confirm the DoD need for new IT standards in coordination with the DoD CIO, the USD(AT&L), and the CJCS.

3. USD(AT&L). In addition to the responsibilities in section 8 of this enclosure, the USD(AT&L):

a. Prescribes policies and procedures for carrying out the DSP in accordance with References (m) and (n).

b. Coordinates on IT standards issues, to include processes, procedures, and compliance with the DoD CIO, the CJCS, and the DoD EA for IT Standards.

c. Oversees IT standards compliance in accordance with section 7 of Enclosure 3 of this instruction.

d. Approves, in coordination with the CJCS and the DoD CIO, the IT standards baselines and updates for inclusion in the DISR.

e. Requires that DoD IT MIL-STDs and specifications listed in the DISR be indexed in the DSP ASSIST database at https://assist.dla.mil/online/start/.

f. Participates in the IT standards waiver process, in coordination with the CJCS and the DoD CIO.

g. Establishes processes and procedures for IT standards compliance for all acquisition programs in accordance with Interim DoDI 5000.02 (Reference (u)).

h. Coordinates with the DoD CIO, the DoD EA for IT Standards, and the CJCS and other DoD Component heads, as required, to establish processes and procedures for IT standards compliance.

DRAFT

4. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO). In addition to the responsibilities in section 8 of this enclosure, 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 the DoD ITSP will be included in appropriate budget-exhibit submissions.

5. USD(I). In addition to the responsibilities in section 8 of this enclosure, the USD(I):

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

b. Directs Defense Intelligence Components to comply and conform with the IT standards in the DISR, pursuant to section 7 of Enclosure 3 of this instruction.

c. Leads the coordination of intelligence enterprise IT across the DoD, the IC, and with multinational partners.

d. Coordinates with the DoD CIO and the IC CIO to develop policy and procedures that apply to the prescription of IT standards for the DoD and the IC.

e. Coordinates with the DoD CIO and the IC CIO to establish a community-based forum and IT standards governance structure to collaborate on common standards, DoD and IC-unique standards, profiles, and other specifications for the respective information environments.

f. 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.

6. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS). Under the authority, direction, and control of the USD(I), in accordance with DoDD 5100.20 (Reference (v)), and in addition to the responsibilities in section 8 of this enclosure, the DIRNSA/CHCSS:

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

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

DRAFT

c. Requires, with the other appropriate DoD Components, the IC, or other U.S. government agencies, that National Security Agency/Central Security Service (NSA/CSS) IT standards profiles for processing foreign intelligence and foreign counterintelligence information will be satisfied by designing and developing interoperable, technical, procedural, and operational interfaces.

d. Requires that NSA/CSS IT programs be certified for standards compliance and conformance.

e. Coordinates with and advises the DoD Components on waivers to cybersecurity standards for NSS, or waivers to SIGINT standards for all IT systems and programs.

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

g. Prescribes the minimum 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 in accordance with Reference (v).

h. Coordinates with the Director, NIST, to ensure NIST standards are complementary to NSS standards, pursuant to section 3543 of Title 44, U.S.C. (Reference (w)).

i. Coordinates with the Committee on NSS (CNSS) to ensure the development of necessary security architectures and to approve the security standards and doctrine for NSS in accordance with CNSS Directive No. 900 (Reference (x)).

7. DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA). Under the authority, direction, and control of the USD(I), in accordance with DoDD 5105.60 (Reference (y)), and in addition to the responsibilities in section 8 of this enclosure, the Director, NGA:

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

b. Identifies, develops, and supports (in coordination with the DoD Components through the GEOINT Standards Working Group) standards, standards profiles, and specifications for GEOINT IT, data, products, and services. This will promote interoperability, information sharing, reuse, portability, and cybersecurity.

c. Promotes the adoption of open (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, standards profiles, and specifications for the National System for Geospatial Intelligence.

DRAFT

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

f. Processes all waivers to this instruction on GEOINT standards in accordance with section 8 of Enclosure 3 of this instruction.

g. Coordinates with the DoD CIO, the USD(AT&L), the DoD EA for IT Standards, and the CJCS and other DoD Component heads to establish processes and procedures for enforcing GEOINT standards compliance.

8. OSD AND DoD COMPONENT HEADS. The OSD and DoD Component heads, in addition to other responsibilities established this enclosure:

a. Require that IT and NSS are in compliance with standards of the U.S. government and DoD. Require program managers for IT acquisitions and procurements include standards views compliant with the DoD Architecture Framework (Reference (z)) and a summary list of all system interfaces in the architectural artifacts within the ISP in accordance with DoDD 8330.01 (Reference (aa)).

b. Oversee the use of mandated DoD IT standards profiles when developing or upgrading IT to support system interoperability.

c. Require that all IT complies with the IT standards in the DISR, or get a waiver in accordance with section 8 of Enclosure 3.

d. Fully support the ITSP through planning, budgeting, execution, and identification of costs in support of the ITSP.

(1) Direct representatives, as appropriate, to perform their responsibilities in support of DoD IT Standards Governance Structure as described in Enclosure 3.

(2) Coordinate with the Director, DISA in developing programmatic and technical guidance, including IT standards and standards profiles for inclusion in ISPs in accordance with Reference (aa). Follow the procedures and best practices as described in the Defense Acquisition Guidebook (Reference (ab)).

(3) Submit change requests for adding, deleting, or revising standards in the DISR.

(4) Participate in configuration management of the DISR.

(5) Participate in SDO and standards setting organization (SSO) open standards development efforts to influence development of IT standards that satisfy DoD requirements to enable interoperability, information sharing, reuse, portability, and cybersecurity.

e. Request waivers to this instruction in accordance with section 8 of Enclosure 3.

DRAFT

f. Use IT standards in the DISR for system development, acquisition, and procurement, considering impacts to cost, schedule, performance, and cybersecurity.

g. Establish, as required, formal standards conformance certification for connection to DoD Component-owned IT systems.

h. Approve waivers to use other than mandated or emerging standards in accordance with paragraph 8a of Enclosure 3.

i. Coordinate with the DoD CIO, the USD(AT&L), the DoD EA for IT Standards, and the CJCS, as needed, to establish processes and procedures for enforcing IT standards compliance.

j. Provide representatives to the JESC in accordance with Reference (i), as appropriate.

9. CJCS. In addition to the responsibilities in section 8 of this enclosure, the CJCS:

a. Confirms, in coordination with the DoD CIO, the USD(AT&L), and the Director DISA, that DoD Architecture Framework (DoDAF)-compliant IT standards viewpoint data is included in Joint Capabilities Integration and Development System (JCIDS) documentation. DoDAF-compliant IT standards viewpoint data will be prepared in accordance with Reference (z). Processes for inclusion in JCIDS documentation are described in CJCS Instruction 3170.01H (Reference (ac)).

b. Provides a sufficiency assessment of IT standards and standards profiles to meet military requirements.

c. Provides the DoD CIO with military priorities for development and adoption of IT standards and profiles.

d. Coordinates with the DoD CIO, the USD(AT&L), the DoD EA for IT Standards, and the other DoD Component heads, as required, to establish processes and procedures for enforcing IT standards compliance.

e. Confirms any DoD need for new IT standards, in coordination with the DoD CIO, the USD(AT&L), and the Director, DISA.

f. Participates in the IT standards waiver process, in coordination with the DoD CIO and the USD(AT&L).

g. Approves, in coordination with the DoD CIO and the USD(AT&L), the IT standards baselines and updates for incorporation in the DISR.

h. Provides representation, in coordination with the other DoD Component heads, to multinational IT standards organizations.

DRAFT

i. Represents CCMD concerns in all aspects of the ITSP.

DRAFT

ENCLOSURE 3

PROCEDURES

1. PURPOSE. This enclosure provides procedures for management and administration of IT standards life-cycle, governance, SDO management, adoption and development, management, compliance and conformance, and waivers.

2. IT STANDARDS LIFE-CYCLE. Operational requirements drive the IT standards life-cycle. Accredited, open (voluntary consensus) standards considered for use in the DoD will be developed in the public and private sectors with Federal Government participation. DoD then selects standards for inclusion in the DISR. When requirements cannot be satisfied from available IT standards, the DoD develops its own unique specifications, as needed, in accordance with References (n) and (o), for inclusion in the DISR. IT standards will be periodically evaluated for their currency and relevancy. IT standards are categorized as emerging, mandated, retired, and sunsetted. These IT standard categories are defined in the Glossary.

3. DoD IT STANDARDS GOVERNANCE. The DoD CIO, in coordination with the IC CIO, has established a joint governance structure to direct, oversee, and set priorities for prescribing IT standards across the DoD and the IC.

a. IT standards procedures will be developed by the DoD EA for IT Standards and will address:

(1) IT standards usage guidance, instructions, and documentation.

(2) Proper criteria for IT standards registration, adoption, and content management.

b. The governance structure used for identifying, developing, and prescribing IT standards in the DoD consists of the JESC, its associated Executive Steering Group (ESG), and Technical Working Groups (TWGs).

(1) JESC. The JESC will be subordinate to an appropriate forum of the CIO EB to be determined by DoD CIO. The JESC serves as the DoD and IC enterprise IT standards governance body responsible for collaborating and recommending common standards, standards profiles, and specifications for the respective DoD and IC information enterprises. The JESC is governed by its charter, which is cosigned by the DoD CIO and the Assistant Director of National Intelligence and IC CIO.

(a) All the DoD Components will provide representatives pursuant to Reference (i), as appropriate.

(b) The JESC selects, approves, and adopts standards for inclusion in the DISR.

DRAFT

(c) Pursuant to Reference (i), the JESC:

1. Coordinates with mission partners to develop specifications and profiles.

2. Advises and supports the DoD and IC CIOs on enterprise standards, profiles, and specifications related to data, services, networks, and security that impact the DoD and IC.

3. Advises the DoD and IC CIOs to more efficiently and effectively manage the development and use of enterprise standards, profiles, and specifications.

4. Recommends IT policies and procedures across the DoD and IC to promote specified enterprise standards, profiles, and specifications.

5. Prioritizes standards activities against mission needs and strategic direction of the DoD JIE and IC IT Enterprise.

6. Supports enterprise architectures through technical standards and profiles.

7. Promotes application of common enterprise standards, profiles, and specifications across the DoD and IC enterprises.

8. Reduces the resource demands for developing, approving, and using common enterprise standards, profiles, and specifications for the DoD and IC.

9. Requires interoperability and scalability among the DoD, IC, and other federal and State agencies (law enforcement, emergency response, and humanitarian relief), wherever possible.

(2) JESC ESG. The co-chairs of the JESC will establish an ESG, consisting of members from both the DoD and IC, to offer leadership, guidance, and management direction to the JESC and TWGs as determined by Reference (i).

(3) TWGs. The JESC will establish TWGs and ad-hoc working groups, as required, to review and propose new standards or update existing standards in the DISR. The number of TWGs and ad-hoc working groups will be kept at a minimum to support efficient and effective review of standards. The co-chairs of the JESC will appoint the TWG chairs.

4. IT SDO MANAGEMENT. The DoD EA for IT Standards will track and report IT standards development and emerging technologies of interest to the DoD. The primary document used will be the annual SDO membership package. The SDO membership package will identify DoD representation and resource needs for participation in external federal, national, and international SDOs and SSOs.

DRAFT

5. IT STANDARDS ADOPTION AND DEVELOPMENT

a. Adoption of IT Standards

(1) Standards will be chosen from the source categories identified in the Table.

Table. DoD Standards Consideration

Source	Example
Federal Law, Regulation, or Instruction	U.S. Code, OMB Circular
Internationally Accredited and Treaty Based	International Standards Organization (ISO), International Electrotechnical Commission (IEC), United Nations/Economic Commission for Europe (UN/ECE), International Telecommunication Union (ITU), International Standardization Agreement
National	American National Standards Institute (ANSI)
Professional Society, Technology Consortia, Industry Association	Institute of Electrical and Electronics Engineers, Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Organization for the Advancement of Structured Information Standards (OASIS), Object Management Group, Open Geospatial Consortium
Federal	Federal Information Processing Standard
Military	MIL-STD, standardization agreement

(2) These attributes and characteristics will be considered by the JESC when selecting standards for inclusion in the DISR.

(a) Utility: Primary features and functions of this standard meet requirements.

(b) Interoperability: Standard meets requirements to connect, access, and share applications and services.

(c) Technical Maturity: Standard is established, stable, and has well-established marketplace support.

(d) Implementability: Standard is used in applications within the federal or private sector.

DRAFT

(e) Security: Standard does not introduce unacceptable cybersecurity risks to the environment.

(f) Applicability: Standard is relevant and meets the needs of programs to include potential risks, impacts on cost, schedule, performance, and security.

(g) Intellectual Property Rights: Standard is publicly available and includes provisions requiring that owners of relevant intellectual property have agreed to make that intellectual property available on a non-discriminatory, royalty-free, or reasonable royalty basis to all interested parties.

(h) Public Availability: Standard is publicly accessible for unrestricted use.

b. New Standards Development. If no existing standard can meet mission needs, a new standard will be developed.

(1) The DoD EA for IT Standards, in coordination with DoD CIO, the USD(AT&L), the CJCS, and the appropriate TWG, must confirm the DoD's need for a new standard.

(2) New standards may be developed either by external public and private sector standards bodies or internal DoD standards development processes contained in References (s) and (t).

(3) The DoD EA for IT Standards, in coordination with the DoD Components, collaborates with military and external federal, national, and international standards bodies to identify and confirm technology trends and emerging standards requirements.

(4) The DoD EA for IT Standards decides whether to pursue either an external public or private sector, or an internal DoD standard development effort. For internal DoD-unique standards development, the DoD EA for IT Standards:

(a) Establishes a DoD PA in accordance with Reference (t), to develop the standard.

(b) Informs all DoD Components and the IC on progress, development, and issues.

(5) The DoD EA for IT Standards transmits to OMB, through the NIST, an explanation of the reason for using government-unique standards in lieu of voluntary consensus standards.

6. IT STANDARDS MANAGEMENT

a. The DoD EA for IT Standards manages a life-cycle process for identifying, developing, and prescribing IT standards. Through this process, standards will be identified as emerging, mandated, retired, or sunsetted.

b. The JESC:

DRAFT

(1) Schedules frequent technical exchanges with IT standards developers, users, and DoD Component and IC Element representatives to verify that IT standards are current, relevant, and complete.

(2) Coordinates with the DoD and IC Components to recommend classification and life-cycle designation of IT standards.

(3) Decides whether to elevate the standard to the next stage of the life-cycle (e.g., emerging to mandated or mandated to retired).

c. When multiple versions of the same standard have been mandated in the DISR, for mission support or operational usefulness, the JESC will decide which version has precedence.

d. The DoD CIO, the CJCS, and the USD(AT&L) will approve periodic IT standards baselines and updates.

7. IT STANDARDS COMPLIANCE AND CONFORMANCE

a. Use of Mandated Standards. Program managers and developers will use IT standards in the DISR for IT system development, acquisition, and procurement to promote interoperability, information sharing, reuse, portability, and information security. If significant negative impacts to cost, schedule, performance, or information security are identified, a system program manager may submit a waiver to use other than DISR-designated "active" standards (e.g., emerging, mandated, and sunsetted), in accordance with section 8 of this enclosure.

b. Use of Mandated Standards Profiles. IT system development, acquisition, and procurement must conform to all applicable mandatory standards profiles in the DISR or derived from the DISR.

c. IT Standards Compliance. Several DoD capabilities, acquisition, and interoperability processes include IT standards reviews. DoD Component program managers must include DoDAF-compliant standards viewpoint data, along with proper systems and services viewpoint data to show where these standards are used, in applicable documentation supporting the:

(1) JCIDS process, in accordance with Reference (ac).

(2) Defense Acquisition System in accordance with DoDD 5000.01 (Reference (ad)) and Reference (u) processes.

(3) IT interoperability certification process, in accordance with Reference (aa).

(a) The DoD EA for IT Standards assesses all DoDAF-compliant standards viewpoint data and provides comments as part of the ISP review process.

DRAFT

(b) The DoD Components must evaluate standards compliance, as a part of the ISP review and approval process, and confirm that waivers required by this instruction are included in the ISP.

d. IT Standards Conformance. Standards conformance occurs through testing to confirm that a product or system adheres to a defined standard, standard profile, or specification.

(1) The DoD Components must conduct appropriate levels of standards conformance testing in the developmental and integration test process. In cases of mature systems, no additional conformance testing may be needed.

(2) The DoD Components operating IT systems (including networks and enterprise services) may call for formal standards conformance certification of external IT systems before connection. System program offices (or developers) desiring connection with these systems will be responsible for funding required standards conformance test and certification (e.g., radio wave conformance, data links, geospatial intelligence).

8. WAIVERS TO DoD IT STANDARDS POLICY

a. OSD and DoD Component heads may approve, in coordination with the DoD CIO, waivers to use other than mandated or emerging standards for acquisition programs where the Component head is the MDA. On approval, the DoD Component will post the waiver to the GTG-F online portal (https://gtg.csd.disa.mil).

b. The DoD CIO, in coordination with the USD(AT&L), the CJCS, and the DoD EA for IT Standards, as appropriate, approves all other waivers to this instruction.

(1) Requests for waivers must be submitted to the DoD CIO for approval. If the request for waiver or any supporting information is classified, the requesting DoD Component must coordinate with the DoD EA for IT Standards for submission procedures.

(2) Requests for waivers must include a DoD Component-level endorsement; the reasons for the waiver, including any negative impacts to cost, schedule, or performance; information security impacts of complying with this instruction; and any operational limitations that will occur if the waiver is granted.

(3) The Director, DISA will review all waivers to this instruction requiring DoD CIO approval. The Director, DISA will analyze these waivers and provide a recommendation to the DoD CIO within 15 calendar days of the waiver request.

c. Waivers may be either permanent or temporary, at the discretion of the approving authority.

d. Before granting a waiver to policy, the approving authority will coordinate with:

DRAFT

(1) The Director, NGA, if a waiver affects implementation of GEOINT standards.

(2) The DIRNSA/CHCSS, if a waiver affects implementation of either cybersecurity standards for NSS or SIGINT standards.

DRAFT

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ANSI	American National Standards Institute
ASSIST	Acquisition Streamlining and Standardization Information System
CCMD	Combatant Command
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CNSS	Committee on National Security Systems
DBS	defense business system
DIRNSA//CHCSS	Director, National Security Agency/Chief, Central Security Service
DISA	Defense Information Systems Agency
DISR	DoD IT Standards Registry
DoDAF	DoD Architecture Framework
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
DSP	Defense Standardization Program
EA	executive agent
EB	Executive Board
ESG	Executive Steering Group
GEOINT	geospatial intelligence
GTG-F	Global Information Grid Technical Guidance Federation
IC	Intelligence Community
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Standards Organization
ISP	information support plan
IT	information technology
ITSP	Information Technology Standards Program
ITU	International Telecommunication Union
JCIDS	Joint Capabilities Integration and Development System
JESC	Joint Enterprise Standards Committee
JIE	Joint Information Environment
LSA	lead standardization activity

DRAFT

MDA	Milestone Decision Authority
MIL-STD	military standard
NGA	National Geospatial-Intelligence Agency
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSS	National Security Systems
OASIS	Organization for the Advancement of Structured Information Standards
PA	preparing activity
SDO	standards development organization
SIGINT	signals intelligence
SOP	standard operating procedure
SSO	standards setting organization
TWG	technical working group
UN/ECE	United Nations/Economic Commission for Europe
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer
USD(I)	Under Secretary of Defense for Intelligence
W3C	World Wide Web Consortium

PART II. DEFINITIONS

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

accredited standard. A published standard from a recognized SSO (e.g., ISO, IEC, ITU, UN/ECE, ANSI). Includes responsible SDOs that have an established position within the relevant technical, professional, and marketplace communities as an objective authority in its sphere of activity (e.g., IETF, W3C, OASIS).

approved IT standards. Consists of mandated, emerging, sunsetted, and retired IT standards in the DISR.

ASSIST. Defined in Reference (t).

DBS. Defined in section 2222 of Reference (c).

DISR. A registry that provides a set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to direct that a conformant

DRAFT

system satisfies a named set of requirements. It defines the service areas, interfaces, standards (registry elements), and standards profiles applicable to all DoD systems. Use of the registry is mandated for the development and acquisition of new or modified fielded IT systems throughout the DoD. The DISR is accessed through the GTG-F portal at https://gtg.csd.disa.mil.

emerging standard. A standard that may replace an existing mandated standard at some point in the future.

enterprise architecture. Defined in Reference (q).

GEOINT. Defined in Reference (y).

interoperability. Defined in Reference (aa).

IT. Defined in section 11101 of Title 40, U.S.C. (Reference (ae)).

IT standard. Technical definitions for information system processes, procedures, practices, operations, services, interfaces, connectivity, interoperability, information formats content, interchange, and transmission or transfer. IT standards apply during the development, testing, fielding, enhancement, and life-cycle maintenance of DoD information systems.

ITSP. Describes the process for the DoD EA for IT Standards to lead, manage, join, and coordinate DoD efforts to promote interoperability, information sharing, reuse, portability, and cybersecurity.

JCIDS. Defined in Reference (ac).

JESC. Defined in Reference (i).

LSA. Defined in Reference (t).

mandated standard. A standard, specification, or profile that is accredited or an open (voluntary consensus) standard that will be required for the development and acquisition of IT systems. The process to adopt and develop mandated standards is contained in section 5 of Enclosure 3 of this instruction. DoD-mandated standards will be listed in the DISR to be selected by programs as part of their acquisition milestone preparation process or when upgrading fielded systems.

NSS. Defined in section 3542 of Reference (w).

open (voluntary consensus) IT standard. A standard that is prepared by authoritative consensus bodies and that is publicly available with patents, copyrights, intellectual property right constraints, and royalty provisions; and intellectual property contained therein is made available on a non-discriminatory, royalty-free, or reasonable royalty basis to all interested parties.

PA. Defined in Reference (t).

DRAFT

retired standard. A standard that will no longer be used in new or upgraded systems. All retired standards citations remain in the DISR archive.

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.

service. Defined in Reference (u).

specification. An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.

standard. Defined in Reference (o).

standard citation. The metadata regarding each IT standard in the DISR. The DISR does not hold engineering specifications. This metadata includes information on the purpose and use of the standard and information on where the full standard is recorded.

standards compliance. The verification and validation that documentation, such as JCIDS documents or ISPs, for a system, product, IT service, or interface complies with the policy in this issuance.

standards conformance. Confirmation by testing that a system, product, IT service, or interface adheres to a standard, standards profile, or specification.

standards profile. A set of one or more base standards, and, where applicable, the identification of chosen classes, subsets, options, and boundaries of those base standards necessary for accomplishing a particular function.

standards validation. Validation to decide if the standard itself is complete, correct, and internally consistent.

sunsetted standard. A status that may be assigned to a mandated standard based on a predefined event or date for future retirement. Program developers may choose to declare use of the sunsetted standard without submission of a waiver but will be expected to migrate to the appropriate emerging standard once it achieves mandated status and the associated sunsetted standard is fully retired.

DRAFT