|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Policy Type | Policy | Partner Org”s | Overview | Status |
| Air Force Directive | ECRETARY OF THE AIR FORCE MISSION DIRECTIVE 1-26 14 JUNE 2023 | Air Force | A1.35. Authority for enabling a secure sharing environment in the DAF that supports the warfighting, business, DoD intelligence, and enterprise information environment mission areas, as delegated to the SecAF pursuant to DoDI 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense. | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| Air Force Manual | SECRETARY OF THE AIR FORCE MANUAL 14-401 26 MAY 2021 | Air Force | INTELLIGENCE ANALYSIS AND TARGETING TRADECRAFT / DATA STANDARDS 2.1.5. Appoint an Air Force ISR Chief Data Officer to establish ISR-specific guidance, standards, data-centric architecture, and procedures to manage data during its life cycle to meet Intelligence Community, DoD, and DAF requirements outlined in ICD 121, ICD 501, ICD 503, DoD Instruction (DoDI) 8310.01, Information Technology Standards in the DoD, DoDI 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense, DoDI 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense, and DoD Directive (DoDD) 5250.01, Management of Intelligence Mission Data (IMD) in DoD Acquisition. (T-0). 2.6.6. Establish and resource an ISR senior data officer to implement and manage NASIC specific data standards and oversee proper life cycle management, storage, cataloging, and tagging of all data of intelligence value per ICDs 121, 501, and 503, DoDIs 8310.01, 8320.02, and 8320.07, and DoDD 5250.01. (T-0). As required, identify subordinate units needing ISR data portfolio leads and coordinate with other senior data officers and the Air Force ISR Chief Data Officer to effectively manage ISR-specific data. (T-1). 2.9.6. Establish and resource an ISR senior data officer to implement and manage ISR specific command data standards and oversee proper life cycle management, storage, cataloging, and tagging of all data of intelligence value per ICDs 121, 501, and 503 and DoDIs 8310.01, 8320.02, and 8320.07. (T-0). As required, identify subordinate units needing ISR-specific data portfolio leads and coordinate with other senior data officers and their \respective service ISR Chief Data Officer to effectively manage ISR-specific data. | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| Army Regulation | Army Regulation 25-1 Army Information Technology 15 July 2019 | Army CIO | *(a)* Army organizations will consider a “NIEM-First” strategy in accordance with DODI 8320.07 for new system and systems being modernized when developing an XML-based information exchange specifications. *(b) When NIEM is not the most efficient or effective means to address an information-sharing requirement, organiza-tions will document the technical, fiscal, and operational reasons why the alternative approach is better and will submit a request for an exception to the “Consider NIEM-First” policy to the DOD–CIO, as described in DODI 8320.07.* | Army CIO is currently working with NIEMOpen to establish a Land domain. The intent is to convert the current U.S. Army use of the MIP Information Model (MIM) to be NIEM conformant. |
| Coast Guard | COMDTINST 5200.7A COAST GUARD ENTERPRISE DATA MANAGEMENT (EDM) POLICY | Coast guard | Enterprise Data Architect. Responsible for oversight and guidance for the enterprise data architecture, including data models and standards, metadata management, data sharing architecture (Data Reference Model (DRM), National Information Exchange Model (NIEM)) and data governance | Cited in responsibilities section. |
| DCMA Manual | DCMA Manual 4502-15 Enterprise Data Governance April 1, 2022 | DCMA | Major Changes to Data Structure. Proposed major changes and customizations to authoritative data sources, and new data structures that impact interfaces and integration must be reviewed. (See Paragraphs 3.2.a. through 3.2.h.) The review must include a conformity analysis summary pursuant to Enclosure 3, DoD Instruction (DoDI) 8320.07, “Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense,” Paragraphs 3.a. through 3.f. All major changes must be communicated to the Agency’s data consumers. 5.4. AUTHORITATIVE DATA SOURCES. DCMA will use authoritative data sources established through regulations, policy, public law, etc., as the basis for validating data requirements to eliminate redundancy, ambiguity, and increase data sharing IAW DoDI 8310.01 and DoDI 8320.07 | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| MILSTD | MILSTD 6017 Variable Message Format (VMF) | DoD | Development of a NIEM Conformant variant of VML |  |
| DoDI | DODI 8320.07 Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense | DoD CDAO | “…the use of NIEM-based exchanges must be considered for all new Extensible Markup Language (XML) information exchanges created and for all XML information exchanges being modernized as part of the normal lifecycle management for these information exchanges. | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| DoDI | DoD Instruction 8170.01 ch 1, Aug 2021 Online Information Management and Electronic Messaging | DoD CIO | Section 3.11 Data b. Architect new DoD electronic messaging services for openness and expose high-value data and content as Web APIs at a discrete and digestible level of granularity with metadata tags, in accordance with the May 23, 2012 Federal CIO Memorandum and the tagging concepts and standards found in DoDI 8320.07 | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| DODI | DoD Instruction 8420.02, "DoD Satellite Communications," August 3, 2023 | DoD CIO | Section 1.2 Policy f. Data from DoD IS, DODIN-connected NSS, and DODIN-connected systems supporting NSS, including, but not limited to, fault, configuration, performance and security data, will be shared and exchanged through common interoperable standards in accordance with DoD Instruction (DoDI) 8320.02 and direction from United States Cyber Command (USCYBERCOM). | Indirect recognition to comply with DoDI 8320.07 NIEM First policy via compliance with DoDI 8320.02. |
| DoDI | DODI 5525.16 Law Enforcement Defense Data Exchange (LE D-DEx) | DoD CIO | Instruction establishes policy and assigns responsibilities for law enforcement criminal justice information (CJI) sharing through the LE D-DEx, by the law enforcement agencies (LEAs) of DoD in accordance with the authority in DoD Directive 5525.21. Information is obtained using the NIEM based exchanches with National Data Exchange N-DEx system. | Current implementation via interface with DOJ N-Dex data system |
| DODI | DoDI 8110.01, "Mission ,PArtner Environment Information Sharing Capability Implmentation for the DoD," Effective June 30, 2021 | DoD CIO | Section 1.2 Policy (1) Pursuant to DoDI 8320.07, the National Information Exchange Model must be considered when deciding which data exchange standards or specifications meet mission and operational needs. Section 4.3. DODIN TRANSPORT SECURITY MANAGEMENT c. Share DODIN situational awareness data with USCYBERCOM and other DoD Components in accordance with DoDI 8320.02, DoDI 8320.07, DoDI 8410.02, and DoDI 8410.03. | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| DODI | DoDI 8310.01, "Information Technology Standards in the DoD," April 7, 2023 | DoD CIO | Several references to 8320.07 | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| DODI | DODI 8330.01 Interoperability of Information Technology (IT), Including National Security Systems (NSS) December 11, 2019 | DoD CIO | Data sharing requirements and use of the Data Services Environment as specified in Reference (r) and DoD Instruction 8320.07 | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| DODI | DoDI 8500.01, Cybersecurity | DoD CIO | Section 7. DOD Information DoD’s information sharing policies and procedures are defined in DoDD 8320.02 (Reference (cr)) and DoDI 8320.07 (Reference (cs)). Information sharing actions and activities will be aligned with the DoD Information Sharing Operational Strategy and Guidance (see www.dodcio.defense.gov). | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| DoDI | DOD INSTRUCTION 8910.01 DOD Implementation of the Paperwork Reduction Act | DoD CIO | DOD Implementation of the Paperwork Reduction Act | In compliance with and directly enables: Section 2.5 OSD and DoD Component Heads, sub-section a.2 Use machine-readable and open data formats, data standards, common core, and extensible metadata for all new information creation and collection efforts. |
| DoDI | DODI 8320.05 Electromagnetic Spectrum Data Sharing | DoD CIO | A community of interest (COI) shall be used as a strategic approach for developing the agreements necessary for meaningful information exchange, and doing so collaboratively across the community of people who share a common interest. An Electromagnetic Spectrum Data COI shall be established and function, in accordance with DoDI 8320.07 (Reference (d)), to ensure spectrum-related data identification, standardization, collection, provision, and maintenance is provided for meeting the needs of the Department of Defense. | Currently working with DISA to make Electromagnetic Spectrum Data NIEM Compliant |
| MILSTD | MILSTD 6016 (Link-16) Tactical Data Link J-series messages XML standardization  STANAG 5516 | Joint Multi-TDL CCB | Approved Draft Interface Change Proposal to develop Appendix to provide guidelines for generation of J-Series message data as NIEM conformant XML | The appendix to 6016 will provide for the conversion of J-series binary messages to XML; and back to binary. One of the primary considerations of this effort is NIEM conformance. |
| JS CJCSM | CJCSM 3265.01A JOINT COMMAND AND CONTROL (C2) REQUIREMENTS MANAGEMENT PROCESS AND PROCEDURES | Joint Saff | Multiple reference to using NIEM |  |
| CJCSM | CJCSM 3265.01A JOINT COMMAND AND CONTROL (C2) REQUIREMENTS MANAGEMENT PROCESS AND PROCEDURES | Joint Staff | Currently reference NIEM section 5.3 Mission Partner Interoperability, Section 7 Data | Currently reference NIEM section 5.3 Mission Partner Interoperability, Section 7 Data |
| JS CJCSI | CJCSI 6610.01F TACTICAL DATA LINK STANDARDIZATION AND INTEROPERABILITY | Joint Staff | Pg. A-6 (2) The DoD adoption of the National Information Exchange Model (NIEM) will serve as the basis for a significant portion of its data exchange strategy, and may facilitate the ability to share information among multinational, interagency, and Service entities. DoD programs will consider and apply NIEM for XML-based message exchanges where it's application is determined to be useful and practical. DOD's strategy includes the Military Operations (MilOps) domain. The MilOps domain which provides shared data definitions, methods, and tools which may be used in multiple formats and standards. |  |
| DoD | Joint All Domain Command and Control (JADC2) | Joint Staff, CDAO, OUSD, DOD MPE Exec Agency | Warfighting Capability intended to Sense, make Sense and Act at all levels and phases of war and across all domains with partners, to deliver information advantage at the speed of relevance. | Currently being implemented through five stable and enduring Lines of Efforts, objectives and tasks to achieve strategic goals. Multiple reafferences to NIEM in the JADC2 RA Enclosure D (JADC2 Capability Development and Analytical Framework) within the Application and services, Interface and Data & Information principals. Also, Refenced at the JADC2 RD Standard View 2. |
| Joint Staff | JSM 5100.06 28 April 2023 ORGANIZATION AND FUNCTIONS OF THE JOINT STAFF DIRECTORATE FOR COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS/CYBER, J- | JS J6 | DSD Responsibilities: Develops, maintains, and supports interoperable C2 data exchange and tactical interoperability standards. (references n and z). Facilitates the harmonization, mediation, and/or migration of data frameworks and standards to the National Information Exchange Model (NIEM). Enables implementation of the NIEM within the DoD. Acts as the NIEM Military Operations (MilOps) Domain Representative Steward and NIEM Management Office lead. (references z, cc, and dd). Establishes, supports, and maintains the NIEM domains and NIEM Management Office. Manages the NIEM MilOps Domain and NIEM governance IAW all applicable DoD policies and NIEM Management Office agreements. Leads NATO Data Management Capability Action Team, generating the NATO Core Data Framework (NCDF) for use by NATO and the FMN program as a STANAG. Provides guidance, processes, and plans to achieve data and standards integration and interoperability. The NCDF focus is on harmonizing the standards related to data exchanges for cross-COI interoperability. (references cc and oo). | Actively managing the the NIEMOpen project, serving as the MILOPS Domain Steward and Leading the NATO Core Data Framework (NCDF), or NIEM in NATO effort. |
| NATO | Integrating NIEM via STANAGs NCDF STANAG 5653 | JS J6, Germany, NATO ACT / NCIA) | Semantics: MIP Information Model (MIM) UML format to NIEM-conformant XML creation. Syntax: NATO XML Naming Design Rules to mimic NIEM | NATO Core Data Framework (NCDF) leverages the NIEMOpen framework Naming and Design Rules, Information Exchange Package Documentation (IEPD) process/format and overall framework components. |
| Marine Corps Order | Marine Corps Order MCO 5230.19A LOGISTICS DATA MANAGEMENT 27 MAR 2017 | Marine Corps | 3.23.7. Consistent with DoDI 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense, identifying data and AI capabilities and aligning them with Department of the Air Force and DoD strategies to develop data-centric investment strategies and to find solutions for areas of concern | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| MILSTD | MILSTD 2525 Symbology STANAG 2019/APP-6 | NATO | Standardized set of graphical symbols for the display of Information in C2 Systems and Applications. | Both U.S. and NATO standards aligned; NIEM v3.0 and v4.0 support exchanging SIDC codes. |
| NATO | STANAG 8517 | NATO | STANAG 4715 is a NATO Standardization Agreement (STANAG) focused on biometric data interchange, watchlisting, and reporting | NATO Automated Biometric Identification System (NABIS) |
| MILSTD | MILSTD 6520 | NATO, Greece | C3B Interim Measure regarding geographical Entities for C3 Standards Addendum 2 to AC/322-N(2017)0092 | Standing |
| DoD | IC Data-Centric Framework and Joint Guidance Plan, 24 Jan 2023 | NSA | The IC Joint Guidance Plan is a living document, reviewed periodically, and based on lessons learned from the mission sprints and refinement of the Data-Centric Framework. | NIEM is mentioned under for data-related activities, “an organization should adopt controlled vocabularies and terminologies”. Also, NIEM is under the reference standards under guidance such as “IC Elements should conform to NIEM standards to enable humans querying” |
| DoDD | DODD 8190.01e Defense Logistics Management Standards (DLMS) | USD (A&S) | Chg.3 Enclosure 2 page 6  Incorporates changes to ASC X12 standards into DLMS in accordance with the NIEM | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| DoDI | DODI 5525.19 DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Databases (TSDB) | USD I&S | DoD’s use of CJI and terrorist screening information retrieved through IMESA for crime prevention, antiterrorism, and implementation of personnel screening. Information retrieved using NIEM exchanges to Query databases such as NCIC (FBI National Crime Information Center) and the Terrorist Screening Database (TSDB) for derogatory information | Currently using NIEM via interfaces with DHS and DOJ systems |
| DODI | DoD Instruction 1322.26, Distributed Learning (DL) | USD P&R | SECTION 4: IMPLEMENTING DL TECHNOLOGY, STANDARDS, AND SPECIFICATIONS b. In addition to adopting existing Defense Information Standards Registry specifications and standards pursuant to DoDI 8320.07, the DoD Components should | Office of the Undersecretary for Defense’s Advanced Distributed Learning (ADL) is the Domain Steward for the NIEMOpen Learning & Development Domain.  Recognition to comply with DoDI 8320.07 NIEM First policy. |
| DODI | DODI 1312.01 Department of Defense Occupational Information Collection and Reporting April 22, 2020 | USD P&R | . The information collected, stored, and maintained in the DoD ODB shall comply with the standards prescribed in DoDI 8320.02, DoDI 8320.07, DoDI 8910.01, DoD Manual 8910.01 (References (d), (e), (f), and (g)), and this Instruction | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| DODI | DoDI 6440.03, June 10, 2011, Incorporating Change 1 on April 15, 2019 | USD P&R | DoD Laboratory Network (DLN) | Recognition to comply with DoDI 8320.07 NIEM First policy. |
| MILSTD | MILSTD 6040 (USMTF) NIEM Conformance approach, STANAG 7149/APP-11 | USMTF CCB | Onboard/Technical Support to transform existing USMTF XML into a NIEM conformant construct. Potential to include 20,000 new data components into the MilOps Domain | USMTF migrating to NIEM XML; anticipate completion FY25; NATO considering consolidated NATO and U.S. MTF once released. |