DEPARTMENT OF THE ARMY
WASHINGTON DC 20310

10 APR 2020

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Mandatory Implementation of Army Data Services Requirements

1. References:

a. Army Regulation 1-1 (Planning, Programming, Budgeting and Execution), 23 May 2016.

b. Army Regulation 70-1 (Army Acquisition Policy), 10 August 2018.

c. Army Regulation 71-9 (Warfighting Capabilities Determination), 15 August 2019.

d. HQDA Execution Order 009-20 (Army Data Plan Implementation in Support of Cloud Migration), 152158Z Nov 2019.

2. To support the National Defense Strategy objective to provide combat-capable military forces needed to deter war and protect the security of our Nation, we must turn data into a strategic asset. In this time of rapid technological change with challenges from adversaries in every operating domain, our data and data sets are the digital ammunition of the future. We must be able to see, understand, and leverage the data in our platforms, systems, applications, and networks in an integrated and consistent manner to improve our operational decision-making and outcomes. These rules apply to all Mission Areas. In particular, these are critical for Army contributions to Joint All Domain Operations and Joint All Domain Command and Control.

3. The enclosure contains a new set of mandatory base principles and standards for the establishment of Data Services Requirements (DSR). Effective immediately, these DSR apply to all Army Programs, with exclusions by request.

4. The USA and VCSA shall have full decision making authorities regarding compliance through the Information Technology Oversight Council meetings and requests.

5. The Chief Information Officer (CIO) is the proponent for policies, processes, and oversight mechanisms to ensure compliance. The ASA(ALT) shall support the implementation of this memo with all acquisition actions and contracting language for new starts and programs identified as non-legacy.

SUBJECT: Mandatory Implementation of Army Data Services Requirements

6. The point of contact for this action is Mr. Gregory L. Garcia, CIO/G6, Chief Data Officer, (703) 697-1279 or gregory.l.garcia.civ@mail.mil.

James C. McConville
General, United States Army
Chief of Staff

Ryan D. McCarthy
Secretary of the Army

Enclosure

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Futures Command
- U.S. Army Pacific
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Africa/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Cyber Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Human Resources Command

Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Superintendent, Arlington National Cemetery
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency

CF:
Director of Business Transformation
Commander, Eighth Army

Enclosure: Mandatory Data Service Requirements

Data Requirements.

The following Data readiness parameters shall be implemented to ensure data interoperability. All data source designs must comply. These standards support the four tenets of data: 1) secure; 2) data sources; 3) data catalog; and 4) data exchange. The initial set of Data Specific standards were published in Reference 1.d. as Annex D to the base order.

Principle DSR-1: Cybersecurity. Verify compliance with DoD Cybersecurity requirements; and Cybersecurity assessment and authorization is about protecting our access and information, to include restoration of information, if necessary. Reference DoD Instruction 8580.1; each DoD information system is required to have an Information System Security Manager (ISSM) and must implement DoD Risk Management Framework (RMF) governed by DoD Instruction 8510.01, for DoD Information Technology (IT).

Principle DSR-2: Data Sources. All data sources must be developed with the objective that the data must be visible, accessible, understandable, trusted, interoperable, and secure (VAUTIS). VAUTIS data sources must be exposed to consumers to gain additional efficiencies.

Principle DSR-3: Data Catalog. Metadata about all Army data assets must be registered in an enterprise data catalog or repository. Compliance is required to Dublin Core Metadata Element Sets and International Standards Organization Metadata Registries requirements.

Principle DSR-4: Data Exchange & Mapping. All Army data sources must be developed with built-in data exchange capabilities. Data mapping must also be implemented to increase efficiency and ease of use of data assets as they are being translated or transformed. At a minimum, programs and initiatives are required to comply with Global Force Management Data Initiative; International Standards for dates; Geopolitical Entities, Names and Codes, Common (GENC); Joint Consultation, Command and Control Exchange Data Model; or Resource Description Framework standards and schemas.

Principle DSR-5: Data Lifecycle Management: Data must be managed across its lifecycle and captured in a data management plan. Managing data requires managing its lifecycle and will be defined by the data owner. Data management practices must account for the data lifecycle.

Service Requirements.

The following Service-readiness parameters shall be implemented on all data assets that are adopted, adapted, developed, procured, or acquired.

Principle DSR-6: Data Visibility. All new and existing applications, systems, or services deemed non-legacy shall expose their data and functionality through service interfaces (for example, OpenAPI specification).

Principle DSR-7: Data Interfaces. All service interfaces, without exception, must be designed to be consumable from external sources and must plan and design to be able to expose the interface to developers.

Principle DSR-8: Code Reuse. All custom software written by the Army or developed with Army funding will be centrally controlled and made available to all DoD, IC and inter-agency partners within the approved Army source code repositories on the Unclassified, Secret, and Top Secret networks in accordance with Army Directive 2018-26 (Enabling Modernization Through the Management of Intellectual Property).

Principle DSR-9: Inter-Process Communication. There will be no other form of inter-process communication allowed: no direct linking, no direct reads of another data store, no shared-memory model, and no back-doors whatsoever. The only Inter-Process communication allowed is intra-system data exchanges or service interface calls over the network. All other requests or methods require CIO approval.

Network Requirements.

The following net-readiness parameters shall be implemented on all systems, applications and data assets that are developed, procured or acquired. They include:

Principle DSR-10: Architecture Support. Support integrated architecture products, including the Joint Common Systems Function List required to assess information exchange and effectively use for a given capability. These products are related to the three architectural views (operational, systems, and technical) and are compliant with the DoD Architecture Framework version 2.0 or its evolution.

Principle DSR-11: All Net-Centric Data Services will comply with DoD Net-Centric Data and Services Strategies, including data and services exposure criteria. This provides the structural architectural "model" and the common terminology that describes how DoD intends to proceed with DoDIN operations for business, warfare, and IT enterprise management. Paragraph two of JCIDS Manual Appendix E to Enclosure D (Content Guide for the Net-Ready KPP) does not exclude Net-Centric Data Services compliance.

Principle DSR-12: DoD Information Network. Comply with applicable DoD Information Network (DoDIN) Technical Guidance and Direction to include DoD IT Standards Registry-mandated DoDIN net centric IT Standards reflected in the Standards View-1, and Functional and Technical Implementation of DoDIN Enterprise Service Profiles necessary to meet the net centric operational requirements specified in the integrated architecture system views. Systems need to conform to various Key Interface Profiles (KIP) based on desired functionality so they can interface properly with the DoDIN. The

Enclosure: Mandatory Data Service Requirements

KIP are the technical specifications that govern access to the DoDIN

Principle DSR-13: Supportability. Comply with Supportability elements to include Spectrum Analysis, Selective Availability Anti-Spoofing Module, and the Joint Tactical Radio System. DoD IA requirements, including IA certification and accreditation, are specified in DoD Directive 8500.01, DoD Instruction 8500.2, DoD Directive 8581.1, and DoD Instruction 8510.01. Satisfaction of these requirements results in system accreditation and the issuance of an authorization to operate. See Defense Acquisition Guide (DAG) Chapter 7.5 for details.