**DEPARTMENT OF THE ARMY**
**CHIEF INFORMATION OFFICER**
**107 ARMY PENTAGON**
**WASHINGTON DC 20310-0107**

**ADD-GOV-DS-021**

SAIS-ADD (25-1rrrr)

2 April 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Data Stewardship Roles and Responsibilities (Fiscal Year 2024)

1. References. See Enclosure 1.

2. Purpose. The Army Chief Information Officer (CIO) issues this memorandum as guidance to the Army for—

a. Managing Department of Defense (DoD) data efficiently and effectively by controlling and protecting data assets (including data products) in transit and at rest, ensuring Army users handle these data assets properly, and adhering to legal, DoD, and Army requirements and guidance (including references 1a, 1b, 1c, 1d, and 1e).

b. Establishing a culture of data-driven decision making, leveraging data to drive business value while aligning with the DoD Data, Analytics, and Artificial Intelligence Adoption Strategy (reference 1a).

c. Supporting continuous improvement of Army data stewardship practices, processes, and technologies to support the CIO's strategic objectives.

d. This memorandum is issued by the authorities of United States Code (U.S.C.): 10 U.S.C., Section 2223(b); 40 U.S.C., Section 11315; 44 U.S.C., Section 3506; and 44 U.S.C., Section 3520 (references 1f, 1g, 1h, and 1i).

3. Background.

a. Over the past four years, the Army has advanced its vision for data management and analytics, incorporating elements of artificial intelligence. This vision encompasses two main areas: Data Management, which includes Data Production and Data Governance, and Data Analytics Activities, which includes Data Product Development and Data Consumption. The Army's efforts in Data Management have focused on assessing data-producing assets and establishing a strong data governance framework to separate data from systems, thereby enabling data-centric interoperability. Through the Army Data Plan, opportunities within the Army Data Catalog (ADC) and Data Platforms have been explored to enhance data collection, protection, storage, distribution, processing, display, and analysis. To address challenges in becoming a data-driven force, the Army is adopting data mesh principles to standardize data

management, orchestration, and analysis, thus improving the speed and precision of data utilization for mission success.

b. This memorandum supports Secretary of the Army Software Modernization Memo (Army Directive 2024-02 (reference 1j)), through the following tasks quoted from the AD:

(1) AD para. 5k(2)(a): “The Army will update the Army Data Plan and related policies to align [with] data mesh principles to enable data centric interoperability in and between enterprise and tactical environments.”

(2) AD para. 5k(2)(d): “Data Stewards and Functional Data Managers will identify the data products needed to execute current and future doctrine as described in the Decision Driven Data CONOPS [reference 1k].”

c. In line with SECARMY’s directive to form a Data-Centric Army, the Army is committed to fostering a decision-driven culture in data and analytics. The Army’s data strategy will be synchronized with the Office of Secretary of Defense (OSD) and The Joint Staff, with ongoing enhancements to data stewardship practices, processes, and technologies. These improvements will span the entire spectrum of Data Management and Analytics to bolster strategic goals in Artificial Intelligence.

d. By delineating data stewardship roles, and the inclusion of Command-Chief Data and Analytics Officers (C2DAOs), this memorandum aligns the Army’s data management initiatives to support secure, efficient, and effective data integration at echelon. This alignment is crucial for the Army to secure and sustain an information advantage.

4. Guidance. Effective immediately upon signature—

a. This memorandum supersedes the CIO memorandum at reference 1l.

b. Mission Area Leads (MAL) will nominate the Mission Area Data Officers (MADOs) in their Mission Area and submit the names to the Army Chief Data and Analytics Officer (CDAO) for approval and appointment within 30 days of a vacancy.

c. The Army CDAO will review individuals nominated by the MALs for the MADO positions. If approved, the CDAO will appoint the MADOs individually through the issuance of appointment memoranda within two weeks of nomination, in accordance with the Army Data Board's Charter. The Army CDAO will review the MADO assignments annually in coordination with the MALs. In the event of any changes, whether at the annual review or otherwise, the nomination/approval process will repeat as described. The Army CDAO will maintain a list of active MADOs.

d. MADOs will—

(1) Identify and issue appointment memoranda for Data Stewards within their respective Mission Areas, indicating data governance authority over identified domains or functional missions.

(2) Send copies of such memoranda to the CDAO and the CIO Data Integration Division.

(3) Ensure that their Data Stewards are properly registered in the Army Data Catalog (ADC).

(4) Reissue appointment memoranda within a month when there are any changes to the Data Steward assignments or the Mission Area domain structure.

(5) Review and update Data Steward appointments as needed at least annually.

e. Data Stewards will—

(1) Evaluate their functional mission and data products to determine what Functional Data Managers (FDMs) are needed to ensure efficient management of data in their domain.

(2) Select and appoint FDMs, documenting with appointment memoranda describing the scope of their responsibility, and provide copies of the memoranda to the CDAO and their MADO for record keeping.

(3) Maintain proper registration of all their FDMs, data sources, and available data products in the ADC.

(4) Reissue appointment memoranda within a month when there are any changes to the FDM assignments or the Data Steward's domain structure affecting FDM assignment.

(5) Review and update FDM appointments as needed at least annually.

f. FDMs will oversee implementation of the data management and analytics lifecycle processes established or adopted by their Data Stewards.

g. Commands have the option to identify a Command CDAO (C2DAO). In order to maintain consistency across the Army, the activity and responsibilities for a role of that name will follow the guidance given in Enclosure 2. There will be a two-way communication channel between the Army-CDAO and each C2DAO.

h. The CDAO, MADOs, Data Stewards, FDMs, System Owners, and C2DAOs will implement their data management roles and responsibilities as further detailed in Enclosure 2.

5. Compliance. MADOs, Data Stewards, FDMs, and C2DAOs will provide quarterly performance reports to the Army CDAO's office and recommend to the Army CDAO any needed revisions to roles and responsibilities for data stewardship during the duration of this memorandum.

6. Duration.

a. This memorandum stays in effect until superseded, rescinded, or incorporated into Army regulation.

b. The Office of the Army CDAO will ensure this memorandum is reviewed no later than 1 October of each calendar year for supersession, rescission, or inclusion in the next edition of Army Regulation 25-1 (Army Information Technology) (reference 1m).

7. Points of contact.

a. Office of the CDAO at usarmy.data.management@army.mil.

b. Mr. Alfred Hull, SAIS-ADD, (571) 279-1690, alfred.hull2.civ@army.mil.

GARCIGA.LEONEL.T.1186170411
Digitally signed by GARCIGA.LEONEL.T.1186170411
Date: 2024.04.02 12:08:40 -04'00'

Encls

LEONEL T. GARCIGA
Chief Information Officer

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 and Africa
U.S. Army Central
U.S. Army North
U.S. Army South
(CONT)

DISTRIBUTION: (CONT)
- 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 Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Human Resources Command
- U.S. Army Corrections Command
- U.S. Army Recruiting Command

Superintendent, U.S. Military Academy
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency
Executive Director, Military Postal Service Agency
Director, U.S. Army Criminal Investigation Division
Director, Civilian Protection Center of Excellence
Director, U.S. Army Joint Counter-Small Unmanned Aircraft Systems Office
Superintendent, Arlington National Cemetery
Director, U.S. Army Acquisition Support Center

CF:
Principal Cyber Advisor
Director of Enterprise Management
Director, Office of Analytics Integration
Commander, Eighth Army

## REFERENCES


a. DoD Data, Analytics, and Artificial Intelligence Adoption Strategy, 27 June 2023. (Available at https://www.ai.mil).

b. DoD CIO memorandum (DoD Data Stewardship Guidebook), 20 October 2021. (Available at https://armyeitaas.sharepoint-mil.us/:f:/r/teams/ADBOKArmyDataBodyofKnowledge/Shared%20Documents/General/DoD%20Data%20Stewardship%20Guidebook).

c. DoD CDO guidance (DoD Data Stewardship Guidebook), 13 October 2021. (Available at https://armyeitaas.sharepoint-mil.us/:f:/r/teams/ADBOKArmyDataBodyofKnowledge/Shared%20Documents/General/DoD%20Data%20Stewardship%20Guidebook).

d. HQDA, CIO/G-6 memorandum (Consolidation of the 18 November 2019 Army Data Plan), 11 October 2022. (Available at https://www.army.mil/article/261114/army_announces_consolidated_data_plan).

e. HQDA, CIO memorandum (Mandatory Implementation of Army Data Services Requirements), 10 April 2020. (Available at https://api.army.mil/e2/c/downloads/2022/04/21/2ee1f1fe/mandatory-implementation-of-army-data-services-requirements-memo.pdf).

f. Information Technology: Additional Responsibilities of Chief Information Officer of Military Departments, 10 U.S.C., Section 2223(b) (1998). (Available at https://uscode.house.gov/browse/prelim@title10/subtitleB&edition=prelim).

g. Agency Chief Information Officer, 40 U.S.C., Section 11315 (1996). (Available at https://uscode.house.gov/browse/prelim@title40/subtitle3&edition=prelim).

h. Federal Agency Responsibilities, 44 U.S.C., Section 3506 (2006). (Available at https://uscode.house.gov/browse/prelim@title44&edition=prelim).

i. Chief Data Officers, 44 U.S.C., Section 3520 (2006). (Available at https://uscode.house.gov/browse/prelim@title44&edition=prelim).

j. AD 2024-02 (Enabling Modern Software Development and Acquisition Practices), 11 March 2024.

k. Mission Command Center of Excellence Combined Arms Center (Decision-Driven Data Concept of Operations), 6 July 2023.

l. HQDA, CIO memorandum (Army Data Governance Roles and Responsibilities), 1 July 2022 (hereby superseded). (Available at https://armyeitaas.sharepoint-mil.us/:b:/r/teams/ADBOKArmyDataBodyofKnowledge/Shared%20Documents/General/Army%20Data%20Roles%20%26%20Responsibilities/Army%20Data%20Governance%20R%26R%20Memo-Final-20220701.pdf).

m. AR 25-1 (Army Information Technology).

n. DCIO memorandum (Department of Defense Data Management Lexicon), 15 June 2020. (Available at https://www.dni.gov/files/ODNI/documents/IC_Data_Management_Lexicon.pdf).

# DATA MANAGEMENT ROLES AND RESPONSIBILITIES

1. Chief Data and Analytics Officer (CDAO).

a. Description. The Army CDAO is a high-level executive responsible for overseeing the data strategy, management, and analytics of the Army. The Army CDAO is responsible for ensuring that data is collected, processed, and analyzed efficiently and effectively, and that insights from this data are used to drive mission outcomes and improve performance across all mission areas.

b. Responsibilities.

(1) Implement appropriate functions of 44 USC §3520(c) (reference 1i) in alignment with the DoD Data, Analytics, and Artificial Intelligence Adoption Strategy (reference 1a) and other relevant strategies.

(2) Develop, promulgate, and oversee implementation of data-related strategies, policies, standards, processes, and governance. These policies govern data management across the entire data lifecycle (from origination to disposition) and cover all types of data regardless of purpose or use.

(3) Manage the Army Data Catalog (ADC) as the Army's central data catalog to support publication and sharing of data assets, as required by 44 U.S.C., Section 3520(c)(3) (reference 1i).

(4) Establish and run the processes for meeting the Army's data product needs.

(5) Update the Army Data Plan and related policies to align with data mesh principles to enable data centric interoperability in and between enterprise and tactical environments, no later than June 2024, in accordance with AD 2024-02 paragraphs 5k(2)(a) and 5k(4)(a).

(6) Represent the Army at Department of Defense CDAO Forums.

2. Mission Area Data Officer (MADO).

a. Description. Responsible for data, data product development, analytics, and the governance and management of data and analytics within a mission area. Nominated by a Mission Area Lead and confirmed by the Army CDAO. MADOs perform executive data management functions for their respective mission areas. MADOs may convene internal forums to oversee and manage data issues specific to their mission area, to be forwarded to the Army Data Board (ADB) as needed. MADOs will appoint Army Data Stewards to focus on specific operational requirements.

b. Responsibilities.

(1) Data management, data product orchestration, analytics, and the governance and management of data assets within a mission area.

(2) Oversight and coordination of the integration of data within and across mission areas, in accordance with the Army Information Technology Architecture.

(3) Data mesh governance, managing and monitoring data mesh domains for scale and coverage.

(4) Review and contribute to the development of data-related aspects of mission area systems portfolio management processes.

(5) Determine how the information domains that each Data Steward oversees are specified.

(6) Designate, assign, and task Data Stewards within their Mission Area, formalizing the assignments with appointment letters.

(7) Ensure registration in ADC of the Data Steward appointments within their Mission Area and maintain proper registration as changes occur.

(8) Define the scope of Data Steward responsibilities.

(9) Maintain awareness of the nature of the digital workforce within their Mission Area. The MADO advocates for filling gaps in the needs of that workforce. Report to the ADB on any digital skills workforce issues within their domain.

(10) Craft and track metrics that reflect the effectiveness of the activity of the Data Stewards under their purview.

(11) Report data issues, data product orchestration, and data management achievements to the ADB and Army CDAO.

3. Data Steward.

a. Description. For their assigned scope of responsibility, Army data stewards establish protection, sharing, and governance guidelines; maintain data names, definitions, data integrity rules, and domain values; ensure compliance with legal and policy requirements, and conformance to data policies and standards; ensure application of appropriate security controls; and analyze and improve data quality. They provide guidance to Functional Data Managers (FDMs).

b. Responsibilities.

(1) General.

(a) Responsible for overseeing data management across their functional area or domain, e.g., complying, setting, and approving guidance (such as laws, regulations, policies, standards, procedures).

(b) Define and maintain data architecture for assigned scope; ensure consistency of data architecture with overall enterprise architecture.

(c) Assist in development of data-related aspects of mission area systems portfolio management processes.

(d) Designate, assign, and task FDMs within their domain, formalizing the assignments with appointment letters.

(e) Ensure registration of the FDM assignments within their domain in ADC and maintain proper registration as changes occur.

(f) Define the scope of FDM responsibilities.

(g) Report to their MADO on any digital skills workforce issues within their domain.

(h) Craft and track metrics that reflect the effectiveness of the activity of the FDMs under their purview.

(i) Be accountable to the MADO of their mission area.

(j) Identify success stories regarding managing, processing, and extracting value from data in their domain, and shares lessons learned with the Army CDAO and the Army data management community. Sharing these lessons learned will inform the enterprise's collective understanding on extracting value from strategic data assets.

(2) Data Initiative Identification.

(a) Coordinate with the MADO and Mission Area Lead to identify and approve data initiatives.

(b) Prioritize initiatives based on their impact to mission objectives and data analytics goals.

(3) Data Identification.

(a) Approve the data and sources that support the mission objectives and data initiatives by leveraging the ADC, and if necessary, identifying new sources (e.g., additional sensors, non-Army data) and the requirements for the new sources.

(b) Maintain knowledge of the information requirements of all priority processes within the Data Steward's domain.

(c) Assess financial impact of data set selection.

(d) Work with their FDMs to identify the data products needed to execute current and future doctrine as described in the Decision Driven Data CONOPS (reference 1k).

(4) Data Collection/Creation.

(a) Approve data collection guidance and processes.

(b) Select data standards (e.g., data format for imagery from sensors) and oversee compliance assurance.

(c) Oversee data collection from existing and new sources to ensure standards and quality requirements are met.

(d) Monitor that any data collected via government contract abides by any extant data-related contract language requirements published by HQDA.

(5) Data Preparation.

(a) Define and approve the curation processes including data quality requirements, metadata requirements, and access control guidance (tiered) for data.

(b) Identify and define data products and authoritative integrated data sets.

(c) Ensure that data quality is maintained for elements of data products and for authoritative data sets.

(6) Data Storage/Integration.

(a) Establish the domain guidance for data storage (e.g., platforms, cloud, backup) and security (e.g., access controls, authorizations).

(b) Work with peer Data Stewards to reconcile and harmonize data products, data objects and data models across information domains.

(7) Data Maintenance.

(a) Govern and approve the process by which data is updated for conformance with defined data quality requirements for mission objectives.

(b) Update access controls and data quality requirements as necessary to adapt/ respond to consumer feedback.

(c) Report data quality for assets within assigned scope.

(8) Data Use.

(a) Identify and manage the use and application (e.g., data analytics, visualizations, artificial intelligence (AI), machine learning (ML)) of data within assigned scope.

(b) Identify/establish security guidance, permissioning rules, and access controls for data within assigned scope.

(c) Oversee adherence to any extant Data Protect Framework guidance published by the Army CIO.

(d) Validate that data analytics projects are registered in ADC.

(e) Monitor and ensure consumer satisfaction with data and its access.

(f) Monitor and ensure proper data products and/or authoritative data sets are being used for mission area priority initiatives.

(9) Data Provisioning.

(a) Select, approve, and oversee fielding of APIs and services that provide data access to consumers for all shared data sets, and IAW any extant API management policy from the HQDA CIO.

(b) Validate that APIs and data access services comply with security guidance.

(c) Encourage use of data standards and data lexicons within their jurisdiction, including enterprise-scoped ones where suitable. For a lexicon, use the DoD Data Management Lexicon (reference 1n) as a starting point, except for individual term definitions overridden by Army policy.

(d) Validate that data products, including their API endpoints, and sets of authoritative data are properly registered in ADC. This applies to both new and legacy data sets.

(e) Establish guidance for metadata tagging that is to accompany shared data while in transit, consistent with Army enterprise and DoD level guidance.

(10) Data Archiving/Disposal.

(a) Handle government records IAW Army CIO data lifecycle management policy.

(b) Map each data asset within their information domain to General Records Schedule (GRS) and Army Records Schedule (ARS) records.

(c) Approve data archiving and disposal periods by considering records management guidance and resource requirements and/or limitations (e.g., funding).

(d) Ensure that FDMs within their domains see that archiving and disposal of those records are done according to data and records management policy.

4. Functional Data Manager (FDM).

a. Description. FDMs are designated by a Data Steward. They implement enterprise and Data Steward domain specific data management policies and maintain the quality of the data within their scope of responsibility, which aligns with or is a subset of the domain of their Data Steward.

b. Responsibilities.

(1) General.

(a) Control, manage (i.e., access, create, modify, store, use) and provide access to data within assigned scope of responsibility.

(b) Secure, protect, and maintain data, within assigned scope of responsibility.

(c) Assign data product custodians to data products within the data domain, and manage the data product lifecycle of these data products with executive authority over the data product development team.

(d) Register in ADC assignees for data stewardship roles within their information domain, at minimum themselves and, if not already registered, the Data Steward to which they report.

(e) Provide data lifecycle information to support data initiatives, including requirements identification, source information, analytics development and registration, consuming processes, and archiving/disposal planning.

(2) Data Initiative Identification.

(a) Recommend and nominate data initiatives and data requirements that can support the mission objectives.

(b) Identify and define analytics efforts to support mission objectives.

(3) Data Identification.

(a) Discover (search and identify) data sets, or data sources that provide data, which satisfy data needs and requirements of missions and initiatives.

(b) Nominate the data sets and sources for Data Steward approval as authoritative data for use to meet mission objectives.

(c) Nominate for Data Steward approval data products needed to execute current and future doctrine as described in the Decision Driven Data CONOPS (reference 1k).

(4) Data Collection/Creation.

(a) Define/propose data collection guidance and processes.

(b) Oversee collection of data from external sources.

(c) Continuously monitor, evaluate, and log data collections.

(d) Ensure collection guidance is met.

(e) Validate that data collected via government contract abides by any data-related contract language requirements published by HQDA.

(5) Data Preparation.

(a) Ensure validated transformation and curation processes are being used.

(b) Oversee the curation/processing of collected data, including creation of curation metadata records. Ensure records are kept.

(6) Data Storage/Integration.

(a) Engage with system and data platform owners to assess and document security control needs for data within their information domain, including user authorizations, access controls, policy decision points, and execution points, for all modes of data access including APIs. Ensure any controls are consistent with DS, MADO, Army CDAO, and DoD policies, and support Zero Trust principles.

(b) Recommend and support the selection of the tools, technology, and platforms for data storage.

(c) Represent the Data Steward and provide input to system owners with respect to data interoperability and integration issues.

(7) Data Maintenance.

(a) Oversee the updating, maintenance, and refreshing of data in source systems and aggregated data platforms within their information domain.

(b) Assess and oversee cleansing and curation of any updates to data.

(c) Monitor the data products and the authoritative data sets within their domain to ensure that quality requirements for mission objectives are maintained.

(8) Data Use.

(a) Direct and record the different uses (e.g., data analytics initiatives, applications) and users of the data.

(b) Register data analytics efforts in ADC.

(c) Recommend to their Data Steward tools and technology within the available capability set to apply/use the data within their information domain.

(d) Monitor and log data provided to consumers.

(e) Solicit, receive, and respond to data consumer feedback, particularly on data quality and data access issues.

(f) Work with system owners to establish and monitor enforcement of permissioning policies for all modes of data access, including APIs.

(g) Implement, and monitor adherence to, any extant Data Protect Framework guidance published by the HQDA CIO.

(9) Data Provisioning.

(a) Ensure that data products and authoritative data sets are discoverable and available.

(b) Oversee responsible individuals in the registration of data sets, including data products and their API endpoints, in ADC. This applies to both new and legacy data sets.

(i) Register newly provided data sets, including data products, within one week of the time the data is available for sharing.

(ii) Register existing data sets, including data products, as soon as possible, doing so in priority order.

(iii) Additionally, register planned data sets or data products when design is complete, with a status designation of "in process".

(c) Maintain a record of usage of provided data sets, including data products.

(d) Engage with system and data platform owners to see that APIs and data services are managed and operated with appropriate security/access controls (e.g., Identity, Credential, and Access Management (ICAM)), IAW any extant data security and API management policies from the Army CIO. Help implement such policy where needed.

(e) Ensure shared data sets, products, and sources are integrated into the data architecture, and the data architecture is represented in appropriate enterprise architecture documentation.

(f) Oversee that data is provided to consumers in standard format (e.g., National Information Exchange Model (NIEM)), as feasible and appropriate.

(g) Monitor that the metadata tagging accompanying shared data in transit meets Data Steward, Army enterprise, and DoD level guidance.

(h) Ensure exchanged data is secure (e.g., Intelligence Community Metadata Standard for Information Security Marking (IC-ISM), encryption).

(i) Continuously monitor data access and report any security concerns or anomalies.

(10) Data Archiving/Disposal.

(a) Evaluate the conditions for data archiving and disposal. Ensure archiving or disposal of data if conditions are met. This may be supported by automation.

(b) Map the Department of Defense and Army Records Management policies to each data asset.

5. System Owner.

a. The system owner is a crucial part of data management for the data sourced by their system. They must ensure that the data stewardship responsibilities listed in the DoD Data Stewardship Guidebook (reference 1b, reference 1c) for “data custodian” are performed. They must have close collaborative relationships with the FDMs and Data Stewards overseeing their system data, to help them enable interfacing of appropriately curated data for use by enterprise stakeholders, and to register complete and accurate metadata for the data sets they source. Section 5b lists the data stewardship-related responsibilities of system owners.

b. Responsibilities.

(1) Operate and manage systems which collect, manage, and provide access to Army data.

(2) Collect, tag, and process data.

(3) Ensure data quality, including the quality of metadata tags and ADC registration data.

(4) Catalog data. Where needed, support registration of data sets, data products, and data services (including APIs) in the ADC.

(5) Grant individual user's access in accordance with laws, regulations, and policies.

(6) Implement dynamic access by linking data to appropriate digital policy rules and by developing interfaces between information systems and dynamic access services. Work with the appropriate FDM to establish and maintain ADC registration of access points.

(7) Comply with applicable DoD and Army cybersecurity standards.

(8) Manage data user access as prescribed and authorized by appropriate data stewards.

(9) Follow data handling and protection policies and procedures established by appropriate data stewards.

(10) Comply with all federal laws and regulations, and DoD and Army policies applicable to the data in their custody.

(11) Elevate concerns and insights to the FDM or data steward.

6. Command Chief Data and Analytics Officer (C2DAO).

a. Description. C2DAOs are assigned by and for a given command and derive their authority from their command structure. They do not produce Army enterprise data policy. Rather, they implement and enforce policy from the Army headquarters data stewardship hierarchy, and report on data and analytics management activity and issues within the command to that hierarchy. From the perspective of the command, they lead data management activity within the command and represent the command's interests.

b. Responsibilities.

(1) Decision Support Management: Drive the use of data analytics to support informed decision-making for the command.

(2) Data Management: Improve command data lifecycle and nominate data and analytic products across the Enterprise.

(3) Align with HQDA Data Stewardship: Coordinate across their command staff, Army MADOs, Data Stewards, and FDMs to support the development of Army Enterprise Business System efforts to ensure their command's AEBS system requirements are captured and produce the data required to support their commanders' data-driven decisions.

(4) Identify Governance Roles: Assist members of the Army headquarters data governance hierarchy to identify individuals or positions to fill governance roles pertinent to their command, particularly Functional Data Managers.

(5) Collaboration and Culture: Build relationships supporting data-driven strategies and contribute to the C2DAO Community of Interest.

(6) Data Literacy and Training: Perform talent management for the command's digital workforce.