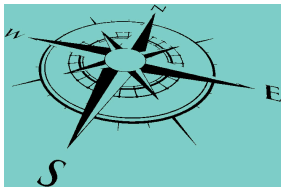
DoD Data Strategy

The DoD Data Strategy, as a key component of the Department's Digital Modernization program, supports the National Defense Strategy (NDS) by enhancing military effectiveness through access to accurate, timely, and secure data.

A core tenet of the DoD Data Strategy is the understanding that data is not an IT asset, but an essential and integral part of the mission itself. Data is ubiquitous. DoD weapons platforms, connected devices, sensors, training facilities, test ranges, and business systems generate enormous volumes of data of which all retain and share their data for broader use. It is critical that data be of high quality, accurate, complete, timely, protected, and trustworthy. As such, the Department makes data a strategic asset by establishing the following goals. DoD data will be:

- Visible - Consumers can locate the needed data.
- Accessible - Consumers can retrieve the data.
- Understandable - Consumers can find descriptions of data to recognize the content, context, and applicability.
- Linked - Consumers can exploit complementary data elements through innate relationships.
- Trustworthy - Consumers can be confident in all aspects of data for decision-making.
- Interoperable - Consumers and producers have a common representation and comprehension of data.
- Secure - Consumers know that data is protected from unauthorized use and manipulation.

Contents



U.S. Department of Defense (DOD)

Stakeholder(s):

David L. Norquist :
Deputy Secretary of Defense

DoD Data Systems :
Scope: The DoD Data Strategy applies to the entire Department of Defense and its data, on whichever systems that information resides.

DoD Leaders :
In addition to combat effectiveness, DoD leaders — including members of the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, Combatant Commands, Defense Agencies, and DoD Field Activities (referred to collectively in this strategy as Components) — require data-driven insights that provide a fair and accurate Department-wide representation of DoD operations and management.

Office of the Secretary of Defense (OSD)

Office of the Chairman of the Joint Chiefs of Staff (CJCS)

Combatant Commands

Defense Agencies

DoD Field Activities

Warfighters :
Warfighters at all echelons require tested, secure, seamless access to data across networks, supporting infrastructure, and weapon systems out to the tactical edge. The advanced capabilities provided by DoD's Digital Modernization program depend upon enterprise data management policies, standards, and practices. Sensors and platforms across all domains must be designed, procured, and exercised with open data standards as a key requirement. Survival on the modern battlefield will depend upon leveraging and making connections among data from diverse sources, using analytic tools for superior situational awareness, and coordinating information for disaggregated-precision effects.

Data Users :
Focus Areas — Data policies and standards alone cannot strengthen data management or improve data quality. They must be continuously informed by feedback from users who consume, produce, manage, and govern data with particular emphasis given to the operational community and warfighter needs. For this reason, the Department must utilize ongoing initiatives in key mission areas to rapidly apply the Strategy's data principles and quickly generate lessons learned. Although data is critical to every DoD mission, initial areas of focus include: Joint All-Domain Operations, business analytics, and senior leader decision support.

Joint Staff :
Joint All-Domain Operations: As part of the National Defense Strategy's focus on great power competition and conflict, the Secretary has directed the Joint Staff and Military Departments (MILDEPs) to develop new concepts for coordinating military effects in an all-domain fight.

Military Departments (MILDEPs)

DoD Data Governance Community :
The data governance community must closely partner with the Joint All-Domain Command and Control (JADC2) Cross-Functional Team (CFT), the Joint Artificial Intelligence Center (JAIC), and the Deputy CIO for C3 to ensure that we can coordinate information with the tactical edge in a highly contested environment. Clear data standards and interoperability requirements for JADC2 directly support future military readiness. The integrated JADC2 exercises led by the Joint Staff will provide real-world outcomes that will aid in prioritizing data gaps, as will lessons from the Army's work on data design principles and similar efforts by the other MILDEPs. When new data gaps are identified, the data governance community must work with mission area managers to determine whether changes are needed to hardware; software; tactics, techniques, and procedures; or risk acceptance. The mitigation of many legacy systems is not cost-effective, making it imperative that all future systems are procured with data-interoperability, software upgradability, and cloud-readiness as requirements.

Joint All-Domain Command and Control (JADC2)

Cross-Functional Team (CFT)

Joint Artificial Intelligence Center (JAIC)

Deputy CIO for C3

DoD CDO :
The DoD CDO, along with Component CDOs, must also ensure that operational users remain informed of new data-enabled capabilities from the commercial sector and DoD research. Ultimately, DoD's transition to a data-centric organization depends on effective feedback between the data governance and operational communities, and the trusted collaboration this entails.

— continued next page

Stakeholders (continued)

DoD Component CDOs

Senior DoD Leaders :
Senior Leader Decision Support: Senior leaders, including the Deputy Secretary, have directed the development of clear, quantifiable metrics to inform a wide-range of management decisions, such as options for implementing the National Defense Strategy. The data community must support efforts to provide current, decision-quality data along with a platform of tools for analysis and visualization. This approach will accelerate the Department's transition to using live, interactive data in place of static slides to inform strategic outcomes.

DoD Comptroller :
Business Analytics: The DoD Comptroller, working with the Chief Management Officer (CMO) and others, is leading an effort to ingest, analyze, and display a wide range of business data; this includes information on budget, procurement, inventory, logistics, and personnel. The data governance community will use the insights from this effort to inform their policies on issues such as authoritative data sources, consistent metadata labeling, standard taxonomies, data provenance, and interfaces (e.g., APIs).

Chief Management Officer (CMO)

DoD Business Analysts :
This effort could also foster migration to a common data platform for all business analytics across the Department.

Vision

DoD is a data-centric organization that uses data at speed and scale for operational advantage and increased efficiency.

Mission

To enhance military effectiveness through access to accurate, timely, and secure data

Values

Principles: Guiding Principles -- The Department leverages eight guiding principles to influence the goals, objectives, and essential capabilities in this strategy. These guiding principles are foundational to all data efforts within DoD.

Strategic Assets: Data is a Strategic Asset -- DoD exerts tremendous effort planning and using traditional strategic assets such as personnel, weapon systems, supply chain, and transportation to achieve positive outcomes. In the same manner, data in the DoD is a high-interest commodity and must be leveraged in a way that brings both immediate and lasting military advantage. As DoD shifts to managing its data as a critical part of its overall mission, it gains distinct, strategic advantages over competitors and adversaries alike. These advantages will be reflected in more rapid, better-informed decisions through the use of trustworthy and integrated data.

Stewardship: Collective Data Stewardship -- To exploit data fully for decision-making, DoD is defining roles and responsibilities for data stewardship. DoD will assign data stewards, data custodians, and a set of functional data managers to achieve accountability throughout the entire data lifecycle. Data stewards establish policies governing data access, use, protection, quality, and dissemination. Data custodians are responsible for promoting the value of data and enforcing policies, and functional data managers implement the policies and manage day-to-day quality.

Ethics: Data Ethics -- The ethical use of data will be at the forefront of all plans and actions for how data is collected, used, and shared. As the Secretary of Defense stated in his guidance on AI Ethics on February 21, 2020, "Although technology changes, the Department's commitment to the Constitution, the Law of War, and the highest standards of ethical behavior does not." Whether for AI or advanced analytics, ethical principles regarding the responsible use of data remain important, and they will be championed by the DoD CDO and all data and analytics leaders across the

Department. Component CDOs will be responsible for promoting a culture of ethical data use supported by oversight mechanisms to identify and promote best practices among the United States and our partners.

Collection: Data Collection -- Regardless of the data domain, community, or use, the challenge remains the same - to discover and collect data and continuously add value to best inform the decision-maker. Consequently, DoD must enable electronic collection of data at the point of creation and maintain the pedigree of that data at all times. The moment data is created, it should be tagged, stored, and cataloged. When the data is combined or integrated, the resulting product must also be immediately collected, tagged, curated, and appropriately secured. To expedite these processes and to minimize the risk of human error, these steps should be automated to the maximum extent possible.

Access: Enterprise-Wide Data Access and Availability -- Closely aligned with data stewardship and collection are the accessibility and availability of data. This is enabled by successful implementation of enterprise capabilities, such as an enterprise cloud; Identity, Credential, and Access Management (ICAM); and associated data-sharing tools. The best technology, processes, and policies will not make this successful if our workforce does not embrace new cultural norms. As such, DoD is making the cultural shift from the need to know (i.e., information withholding) to the responsibility to provide (i.e., information sharing). Making data available across warfighting, intelligence, and business systems is essential to gaining an enterprise-wide view into the daily operations of the Department and absolutely critical to the success of both the National Defense Strategy and the Digital Modernization Strategy. Therefore, it is a fundamental DoD premise that data should be made available for use by all authorized individuals and non-person entities through appropriate mechanisms. To continue this shift, leaders must support this cultural change, set the example, educate their organizations, and enforce data sharing to ensure that the default posture of DoD is to share information broadly. Data sharing should only be restricted when required by law or DoD-wide policy and where security, privacy, or ethical considerations are involved. Furthermore, we must ensure not only that data is protected, but that it is handled properly throughout its lifecycle.

Intelligence: Data for Artificial Intelligence Training -- Artificial Intelligence (AI) is a long-term data competency grounded in high-quality training-quality datasets (TQD) that are the pieces of information and associated labels used to build algorithmic models. TQD and the algorithmic models will increasingly become DoD's most valuable digital assets. As DoD modernizes and integrates AI technologies into joint warfighting, generating DoD-wide visibility of and access to these digital assets will be vital in an era of algorithmic warfare. We must also understand that our competitors gain advantage if these assets become compromised. Therefore, the DoD Chief Data Officer (CDO), in partnership with DoD Components, will create a modern governance framework for managing the lifecycle of the algorithm models and associated data that provides protected visibility and responsible brokerage of these digital assets.

Purpose: Data Fit for Purpose -- Data "fit for purpose" is quality data that is readily discoverable and understood within the context of its intended use. It should include careful consideration of any ethical concerns in data collection, sharing, use, representation of the information intended, rapid data integration, and minimization of any sources of unintended bias. Customers of DoD data have their own requirements for accessing DoD data, which may or may not align with the purpose or intent of the original data collection. Additionally, in some instances, legislation or a regulation may specify how data is to be used and from which source the data must be consumed. The DoD supports data exploration to enhance analyses that impact decision making.

Compliance: Design for Compliance -- Implementation of IT solutions provides an opportunity to automate the information management lifecycle fully, properly secure data, and maintain end-to-end records management. The Department will make data management and compliance with policies a top priority. Compliance with required data policies is a critical success factor for continued funding of future warfighting solutions and will be a gate for authorizations to operate.

1. Visibility

Make Data Visible

The goal of making data visible enables authorized users to discover the existence of data that is of particular interest or value. Data stewards, data custodians, and functional data managers are all responsible and obligated to make their data visible to authorized users by identifying, registering, and exposing data in a way that makes it easily discoverable across the enterprise, and to external partners as appropriate. Moving towards this type of data visibility allows users (person and nonperson entities) to discover and rapidly identify who is responsible for specific data assets, the location of data assets, the types of data assets available, and the means of accessing the data assets. DoD will know it has made progress on making data visible when:

1.1. Advertisement & Availability

Data is advertised and available for authorized users when and where needed

1.2. Metadata

DoD implements metadata standards including location and access methods for shared data.

1.3. Catalogue

All DoD data sources are catalogued.

1.4. Publication, Search & Discovery

DoD implements common services to publish, search, and discover data.

1.5. Visualizations

Warfighting and business governance bodies make decisions based on live visualizations of near real-time data.

Stakeholder(s):

Warfighting Governance Bodies **Business Governance Bodies**

2. Accessibility

Make Data Accessible

The goal of making data accessible enables authorized users to obtain the data they need when they need it, including having data automatically pushed to interested and authorized users. Data accessibility must comply with Public Law (P.L.) 115-435, the Foundations for Evidence-Based Policymaking Act of 2018. DoD is making data, including warfighting, intelligence, and business data, accessible to authorized users. Accessibility requires that protective mechanisms (e.g., security controls) are in place for credentialed users to ensure that access is permitted in accordance with laws, regulations, and policies. DoD will know it has made progress on making data accessible when:

2.1. APIs

Data is accessible through documented standard Application Programming Interfaces (APIs).

2.2. Platforms & Services

Common platforms and services create, retrieve, share, utilize, and manage data.

2.3. Access & Sharing

Data access and sharing is controlled through reusable APIs.

3. Comprehensibility

Make Data Understandable

Understanding data is critical to enable enhanced, more accurate, and timely decision-making. The inability to aggregate, compare, and truly understand data adversely affects the ability of the Department to react and respond. Without proper context, interpretation and analysis of the data could be flawed, resulting in potentially fatal outcomes. Bringing together business and technology and applying a data-centric approach enable massive amounts of data to be transformed into the insights needed to lead DoD more effectively and efficiently. DoD will know it has made progress on making data understandable when:

3.1. Semantics

Data is presented in a way that preserves semantic meaning and is expressed in a standardized manner throughout DoD.

3.2. Syntax

DoD utilizes a common data syntax for the same data types and includes semantic metadata with data assets.

3.3. Dictionary

Data elements are aligned into a comprehensive data dictionary with a controlled, yet flexible, vocabulary and taxonomy.

3.4. Inventory

Data is baselined and inventoried in comprehensive data catalogs with relevant information on purpose, ownership, points of contact, security, standards, interfaces, limitations, and restrictions on use.

3.5. Vocabularies

DoD has processes to create, align, implement, and manage business vocabularies, including enterprise standards.

3.6. Monitoring, Transformation & Insights

Adaptive, intelligent systems monitor data streams and identify opportunities to transform, combine, or derive new data providing increased insights.

4. Relationships & Dependencies

Make Data Linked

Data-driven decision-making requires DoD data to be linked such that relationships and dependencies can be uncovered and maintained. Adhering to industry best-practices for open data standards, data catalogs, and metadata tagging, the Department ensures that connections across disparate sources can be made and leveraged for analytics. DoD will know it has made progress on making data linked when:

4.1. GUIDs

DoD implements globally unique identifiers so data can be easily discovered, linked, retrieved, and referenced.

4.2. Metadata Standards

DoD utilizes common metadata standards that allow data to be joined and integrated.

5. Trust

Make Data Trustworthy

DoD data requires trust to deliver the needed value to its Service members, civilians, and stakeholders. Lacking confidence in the data may result in less timely decision-making or, consequently, no decision when one is warranted. DoD will know it has made progress toward making data trustworthy when:

5.1. Learning & Budgeting

DoD budget requests and the supporting budget process integrate data-focused evidence and Learning Agendas (see P.L. 115-435).

5.2. Protection & Lineage

DoD data has protection, lineage, and pedigree metadata bound throughout its lifecycle.

5.3. Quality

DoD executes data quality management techniques to assess and enhance data quality.

5.4. Data Management

DoD implements master data management for business, intelligence, and warfighting data.

5.5. Records Management

DoD properly tags and maintains all appropriate data and records in accordance with established processes and policies.

6. Interoperability

Make Data Interoperable

Properly exchanging data between systems and maintaining semantic understanding are critical for successful decision-making and joint military operations. Achieving semantic as well as syntactic interoperability using common data formats and machine-to-machine communications accelerates advanced algorithm development and provides a strategic advantage to the Department. DoD will know it has made progress toward making data interoperable when:

6.1. Exchange

DoD documents and implements data exchange specifications for all systems, including those of coalition partners.

Stakeholder(s):
Coalition Partners

6.2. Metadata & Meaning

Exchange specifications contain required metadata and convey standardized semantic meaning with the data set.

6.3. Machine-Readability

Public data assets are machine-readable and available for consumption.

6.4. Mediation

DoD rapidly mediates differing data standards and formats without mission-critical loss of fidelity, precision, or accuracy.

6.5. Tagging Strategy

DoD develops and promulgates a data-tagging strategy and subsequent implementation plan to enable data interoperability.

7. Security

Make Data Secure

As per the DoD Cyber Risk Reduction Strategy, protecting DoD data while at rest, in motion, and in use (within applications, with analytics, etc.) is a minimum barrier to entry for future combat and weapon systems. Using a disciplined approach to data protection, such as attribute-based access control, acrossthe enterprise allows DoD to maximize the use of data while, at the same time, employing the most stringent security standards to protect the American people. DoD will know it has made progress toward making data secure when:

7.1. Privilege Management

Granular privilege management (identity, attributes, permissions, etc.) is implemented to govern the access to, use of, and disposition of data.

7.2. Classification & Compliance

Data stewards regularly assess classification criteria and test compliance to prevent security issues resulting from data aggregation.

7.3. Standards

DoD implements approved standards for security markings, handling restrictions, and records management.

7.4. Markings & Retention

Classification and control markings are defined and implemented; content and record retention rules are developed and implemented.

7.5. Loss Prevention

DoD implements data loss prevention technology to prevent unintended release and disclosure of data.

7.6. Authorizations

Only authorized users are able to access and share data.

7.7. Restriction Metadata

Access and handling restriction metadata are bound to data in an immutable manner.

7.8. Auditing

Access, use, and disposition of data are fully audited.

Administrative Information

Start Date:
End Date:

Publication Date: **2020-10-10**
Source: https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: